Oct. 2022

AICPA® & CIMA®
Together as the Association of International
Certified Professional Accountants

Information for Service Organization Management in a SOC 2® Engagement

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

This document is nonauthoritative and is provided for informational purposes only.

The purpose of this document 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.

Disclaimer: For information about obtaining permission to use this material other than for personal use, please email copyright-permissions@aicpa-cima.com. All other rights are hereby expressly reserved. The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. Although the information provided is believed to be correct as of the publication date, be advised that this is a developing area. The Association, AICPA and CIMA cannot accept responsibility for the consequences of its use for other purposes or other contexts.

The information and any opinions expressed in this material do not represent official pronouncements of or on behalf of the AICPA, CIMA or the Association of International Certified Professional Accountants. This material is offered with the understanding that it does not constitute legal, accounting, or other professional services or advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The information contained herein is provided to assist the reader in developing a general understanding of the topics discussed but no attempt has been made to cover the subjects or issues exhaustively. While every attempt to verify the timeliness and accuracy of the information herein as of the date of issuance has been made, no guarantee is or can be given regarding the applicability of the information found within any given set of facts and circumstances.

Contents

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 include the following:

- Customer support — Providing user entities with online or telephonic post-sales support and service management for their customers. Examples of these services are warranty inquiries and investigating and responding to customer complaints.
- Health care claims management and processing — Providing medical providers, employers, third-party administrators, and insured parties of employers with systems that enable medical records and related health insurance claims to be processed accurately, securely, and confidentially.
- 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.
- eCommerce software-as-a-service (SaaS) application — Providing user entities with shopping cart software, allowing businesses to create an online shop within minutes without coding, hosting, or software.
- Managed security — Managing access to networks and computing systems for user entities (for example, granting access to a system and preventing, or detecting and mitigating, system intrusion).
- Financial technology services — Providing financial services companies with information technology–based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, retirement recordkeeping, crowdfunding, big data analytics, and investment management.
- Environmental, social, and governance (ESG) metric services — Measuring, calculating, and otherwise assisting companies with gathering and reporting their ESG metrics.

Although these relationships may increase revenue, expand market opportunities, reduce costs for the user entities and business partners, and mitigate certain business risks, they also result in new risks arising from interactions with the service organization and its system. Accordingly, the management of user entities and business partners is responsible for identifying, evaluating, and addressing those additional risks as part of its 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 organization and its systems.

To identify, assess, and address the risks associated with a service organization, its services, and the system used to provide the services, user entities and business partners usually need information about the design, operation, and effectiveness of controls[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 service auditor's report is the culmination of an independent service auditor's[2] 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).[3, 4] This examination is referred to as a *SOC 2 examination*.

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

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

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 only the suitability of design of some controls and both the design and operating effectiveness of other controls in a SOC 2 examination.

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

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

[3] As discussed in chapter 2 of 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 guide), 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.

[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 in chapter 1 of the SOC 2 guide.

Intended Users of a SOC 2 Report

A SOC 2 report, whether a type 1 or a type 2 report, is intended to provide report users with information about the service organization's system relevant to security, availability, processing integrity, confidentiality, or privacy to enable such users to assess and address the risks that arise from their relationships with the service organization. The report is also intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with the service organization's system, particularly system controls that the service organization has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria. For example, disclosures about the types of services provided, the environment in which the entity operates, and the components of the system used to provide such services allow report users to better understand the context in which the system controls operate.

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

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations,[5] and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entities' ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

Without such knowledge, users are likely to misunderstand the content of the SOC 2 report, the assertions made by management, and the service auditor's opinion, all of which are included in the report. For that reason, a SOC 2 report is restricted to use by users with that knowledge.

In a SOC 2 report, the following intended users are presumed to have the knowledge identified in the preceding list:

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

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

[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," of the SOC 2 guide discusses these two methods for treating subservice organizations.

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

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

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

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 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's 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

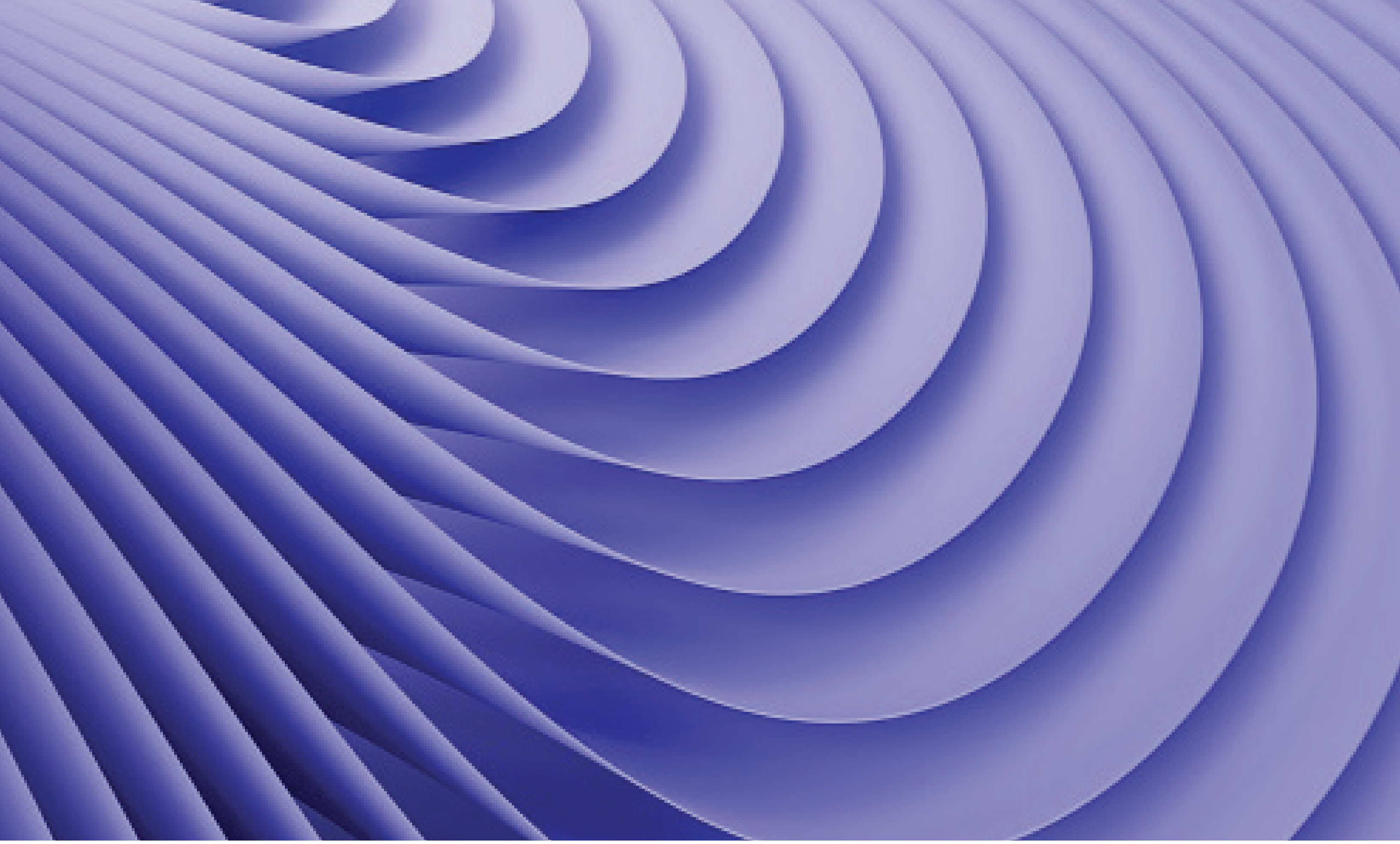
As previously discussed, a SOC 2 examination is an examination of a service organization's description of its system, the suitability of the design of its controls, and, in a type 2 examination, the operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality,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

A service auditor performs a SOC 2 examination in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*,[6] and AT-C section 205, *Assertion-Based 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. 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 guide) 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.[7] 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, which is also included in the SOC 2 report, addresses whether (*a*) the description of the service organization's system is presented in accordance with the description criteria,

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

[7] 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.



(*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 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 (below), the SOC 2 report includes three key components (four in a type 2 examination).

Table 1-1[8]

Contents of a SOC 2 Report

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

[8] This table can also be found in chapter 1, "Introduction and Background," of the SOC 2 guide

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 (With Revised Implementation Guidance — 2022)*,[9] 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 (With Revised Points of Focus — 2022)*,[10] 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

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 guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, users are advised to carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the description criteria.

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.

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

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

The revised implementation guidance is intended to provide users of the criteria with the following:

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

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

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

Trust Services Criteria

The trust services criteria are used to evaluate the suitability of design and operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. Because applying the trust services criteria requires judgment, TSP section 100 also presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control — Integrated Framework* (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.

The current version of the 2017 trust services criteria has been modified to reflect new points of focus and edits to existing points of focus relevant to certain of the trust services criteria. The revisions to the points of focus do not in any way alter the criteria in the 2017 trust services criteria. Such criteria continue to be suitable criteria for use when evaluating the description of a system in a SOC 2 engagement.

The revised points of focus are intended to clarify and better support application of the criteria in

- an environment of evolving, complex technologies and vendor relationships, increasing threats and vulnerabilities, and other matters that may create additional risks to organizations.
- addressing changing legal and regulatory requirements and related cultural expectations regarding areas such as privacy.
- addressing resilience and data management (for example, data storage, backup, retention, and recoverability), particularly when related to availability and confidentiality.
- differentiating which points of focus related to privacy may apply only to an organization that is a data controller or only to an organization that is a data processor, as defined in the trust services criteria glossary. (Although this distinction is intended to assist management and the practitioner in identifying situations in which certain points of focus may be particularly relevant, the specific facts and circumstances of the organization's operations should be considered when identifying and applying points of focus in a trust services engagement.)

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 that manual controls were applied by individuals who have the appropriate competence and authority.

The trust services criteria in TSP section 100 were promulgated by ASEC. ASEC has determined that the trust services criteria are both suitable and available for use in a SOC 2 examination.

Categories of Trust Services 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 services categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

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

Common Criteria

The common criteria presented in TSP section 100, *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 subclassifications: logical and physical access controls [CC6 series], system operations [CC7 series], change management [CC8 series], and risk mitigation [CC9 series].)

ASEC has determined that the common criteria are suitable for evaluating the effectiveness of controls to achieve a service organization's service commitments and system requirements related to security; no additional control activity criteria are needed. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria and (*b*) the control activity criteria applicable to the specific category. Table 1-2 identifies the trust services criteria to be addressed when evaluating the effectiveness of controls for each of the trust services categories and indicates how each category is labeled in the table presented in TSP section 100.

Table 1-2[11]

Criteria for Evaluating The Design And Operating Effectiveness of Controls

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

[11] This table can also be found in chapter 1 of the SOC 2 guide.

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

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

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.

Using the Trust Services Criteria in an Engagement That Addresses Privacy

Some points of focus relevant to criteria in the privacy category may apply only to an organization that is a *data controller* or only to an organization that is a *data processor*. (A data controller is an organization that [alone or jointly with others] determines the purposes for and the means by which personal data is processed. A data processor is an organization that processes personal data at the direction of a data controller. In many cases, a service organization may process personal data for its business-to-business [B2B] customers [user entities], which in turn may function as data controllers. In other cases, a service organization may function as a data controller depending on the facts and circumstances.) This distinction has been noted within the privacy-related points of focus to assist management and the service auditor in identifying situations in which certain points of focus may be particularly relevant. It may also assist management and the service auditor in understanding how the specific facts and circumstances of the organization's operations may affect the identification and application of points of focus in an engagement in which privacy is included in the scope of the examination.

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 identifying its system requirements. Service commitments are the declarations made by service organization management to user entities (its customers) about the system used to provide the service. Commitments can be communicated in written, individualized agreements, standardized contracts, service-level agreements, or published statements (for example, a security practices or privacy statement). Commitments may be made on many different aspects of the service being provided, including the following:

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

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.

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

- Workforce member fingerprinting and background checks established in government banking regulations
- Legal requirements to prevent certain types of transactions
- Entity policies establishing maximum acceptable intervals between periodic review of user 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 the nature of system operation and management's and the service auditor's basis for evaluating the suitability of the design of controls and, in a type 2 examination, the operating effectiveness of controls. Because of the importance of the service commitments and system requirements to the SOC 2 examination, the principal service commitments and system requirements disclosed by management should be appropriate for the engagement.

When considering which service commitments and system requirements are principal service commitments and system requirements, management may consider the following questions:

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

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

- Are the principal service commitments and system requirements complete? For example, in a SOC 2 examination that includes processing integrity, principal service commitments and system requirements would generally be identified related to completeness, validity, accuracy, timeliness, and authorization. An examination based on a complete set of principal service commitments and system requirements can provide intended users with the information they need to assess the effect of the service organization's controls on the risks associated with doing business with the service organization.

Chapter 2, "Accepting and Planning a SOC 2 Examination," of the SOC 2 guide discusses the service auditor's responsibility for assessing whether the principal service commitments and system requirements disclosed by service organization management in the description are appropriate.

Meeting the Requirements of a Process or Control Framework

In some situations, governmental bodies, industry consortiums, or groups of subject matter experts may develop process or control frameworks (for example, International Organization for Standardization and International Electrotechnical Commission [ISO/IEC] Standards 27001 and 27002 or the NIST CSF) for obtaining and sharing specific information from other entities, including service organizations, about a particular subject matter of interest to them (for example, security controls over sensitive information). Most process or control frameworks identify specific sets of processes or controls (referred to in this document as *requirements of the process or control framework*) for entities to implement. In addition, many frameworks establish certification programs to demonstrate that entities have met the requirements of the process or control framework.[12] The most common types of process or control frameworks focus on information security and privacy. In this document, a governmental body, industry consortium, or group of experts that develops and maintains such a framework is referred to as a *sponsoring organization*.

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

When the service organization establishes service commitments and system requirements regarding the requirements of the process or control framework, the evaluation of whether controls were suitably designed and operated effectively would include consideration of whether the implemented controls met those requirements. In this situation, the requirements of the process or control framework are likely to be additional points of focus when using the trust services criteria.[13, 14] For example, a service organization that provides services to a U.S. government entity would likely consider the requirements of the NIST CSF and NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, as additional points of focus when evaluating whether its controls are suitably designed and operating effectively.

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

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

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

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

In other situations, management may include such disclosures in the description of the system. This is likely to be the case when management has identified a principal service commitment or system requirement related to the process or control framework. In this situation, management would generally include information about how the system components, including processes and controls (DC3),[15] addressed requirements of the process or control framework and how the implemented controls met those requirements (DC5).

When management has included disclosures about how the system components, including processes and controls, addressed requirements of a process or control framework and how the implemented controls met these requirements, management would need to ensure the adequacy of those disclosures based on DC3 and DC5, respectively. In addition, the presentation should not be misleading within the context of the engagement. For example, if management indicates that a particular control met a requirement of a process or control framework, and the service auditor determined that the control did not meet that requirement, this could be a material misstatement.

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

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

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

As discussed earlier, there are situations in which a service organization makes commitments about implementing a set of processes or controls to meet the requirements of a specific process or control framework and establishes system requirements to support the achievement of those commitments. If management determines that intended users of the report are likely to want assurance about whether the service organization achieved those commitments and requirements, it may engage the service auditor to also examine and issue a separate opinion about whether the organization has implemented processes or controls to meet the requirements of the process or control framework. In this situation, both management and the service auditor evaluate the controls that management has implemented to meet the objective of the process or control framework (additional criteria) to support management's assertion and the service auditor's additional opinion, respectively. In many cases, the objective of the process or control framework is the implementation of a specific set of processes or controls.[16]

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

In this document, guidance related to SOC 2+ examinations assumes that the service auditor's additional opinion is on whether controls were implemented to meet the requirements of a process or control framework.[17] *Process or control frameworks* are discussed in further detail in the section titled "Meeting the Requirements of a Process or Control Framework."

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

It is likely that the process or control framework is important to a broad range of users and management would identify meeting the requirements of the framework as a principal service commitment or service requirement. Management is also likely to disclose information about how the system components, including processes and controls (DC3), addressed requirements of the process or control framework and how the implemented controls met these requirements (DC5).

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

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

SOC 3 Examination

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

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

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

There is no type 1 equivalent for a SOC 3 report. In a SOC 3 examination, service organization management prepares, and includes in the SOC 3 report, a written assertion about whether the controls within the system were effective[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 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]

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

[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 .A93 of AT-C section 205, *Assertion-Based 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.

Other Types of SOC Examinations: SOC Suite of Services

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

1. SOC 1® — SOC for Service Organizations: ICFR[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
5. SOC for Supply Chain

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. 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.[21] Such an examination is known as a SOC 1 examination, and the resulting report is known as a SOC 1 report. The controls are generally those that a service organization implements to prevent, or detect and correct, misstatements in the information or services it provides to user entities relevant to the financial reporting of the user entity.

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

SOC for Cybersecurity

Cybersecurity has become a top concern for boards of directors and senior executives of many entities, regardless of their size or the industry in which they operate. Government officials are also concerned about cybersecurity at governmental agencies and departments. For most entities, cybersecurity is a significant business risk that needs to be identified, assessed, and managed along with other business risks the entity faces, and it is management's responsibility to ensure that all employees throughout the entity, not only those in the information technology department, address cybersecurity risks. Managing this business issue is especially challenging because even an entity with a highly sophisticated cybersecurity risk management program has a residual risk that a material cybersecurity breach can occur and not be detected in

[20] ICFR stands for internal control over financial reporting

[21] Controls may also 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.

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

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.

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).

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.

SOC for Supply Chain

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

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

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

Management Responsibilities in a SOC 2 Examination Prior to Engaging the Service Auditor

Service organization management is responsible for having a reasonable basis for asserting that (*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. Management's assertion is based, in part, on management having (*a*) identified the service commitments and system requirements, (*b*) identified and analyzed the risks that threaten the achievement of those service commitments and system requirements, and (*c*) designed, implemented, and operated controls that provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria.

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 boundaries of the system
- — Identifying the risks from business partners providing intellectual property or services to the service organization related to the system
- — Selecting the trust services category or categories to be included within the scope of the examination
- — Determining the type (type 1 or type 2) of SOC 2 examination to be performed
- — Determining the period to be covered by the examination or, in the case of a type 1 report, the specified "as of" date
- — If services are provided to the service organization by other entities, evaluating the effect of those services on the service organization's achievement of its service commitments and system requirements and concluding whether those other entities are subservice organizations
- — 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 assessing risks that could prevent the service organization from achieving its service commitments and system requirements
- Designing, implementing, operating, monitoring, and documenting controls that are suitably designed and, in a type 2 examination, operating effectively to provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria
- Identifying known system incidents that
  - — were the result of controls that were not suitably designed or operating effectively or
  - — otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements

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. 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 examination, 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 only a portion of the services? For example, a service organization that provides SaaS 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 agreements.

Definition of a System

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

In the SOC 2 examination, a system is 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 support application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications

- *People.* The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers)
- *Data.* The types of data used by the system, such as transaction streams, files, databases, tables, and other outputs used or processed by the system
- *Procedures.* The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information are prepared

Boundaries of the System

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).

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

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.

It is becoming increasingly common for service organizations to use information provided by third-party software applications or tools, whether installed on the premises or through SaaS, to perform certain internal control activities relevant to the system being examined. For example, tools may assist management in the identification or detection of threats and vulnerabilities (such as firewalls, intrusion-prevention systems [IPSs], intrusion-detection systems [IDSs], and security information and event management systems [SIEMs]); monitoring the implementation of key software settings; or monitoring the effectiveness of automated controls. Such tools would be considered within the boundaries of the system when they support the service organization in achieving its service commitments and system requirements. The processing performed by these tools is designed to be consistent but is highly dependent on other factors such as their configuration, whether the ability to operate and change configuration settings within the tool is appropriately restricted, and whether changes are made in accordance with the change management process. It is important that management consider the risk associated with and information produced by such tools when determining boundaries of the system addressed by the engagement and related disclosures.

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 (such as investment management) or geographical location (like Canadian operations), as long as the personal information is not commingled with information from, or shared with and available to, 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 addition to identifying the components and boundaries of the system, it is also necessary to consider which trust services category or categories are to be addressed by the examination. As discussed previously, 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.

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

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

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

In some situations, the omission of a category that is likely to be important to report users may result in a misleading report. For example, report users may be primarily concerned about cybersecurity risks arising from the interconnection of the service organization's system with users' systems. If service organization management wishes to engage a service auditor to perform an examination addressing only the availability category, such a report could be misunderstood by users, who would expect the examination to address controls designed, implemented, and operated by the service organization to mitigate its security risks, not only those that threaten the achievement of the service organization's availability commitments. In this situation, the service auditor might conclude that an examination addressing only the availability category is likely to be misleading to report users and decide to decline the engagement. Written agreements may provide information on which category or categories should be included within the scope of the SOC 2 examination.

Difference Between Privacy and Confidentiality

As used in this document, the term *confidentiality* applies to various types of sensitive information,[22] whereas *privacy* applies only to personal information[23] and embodies the unique considerations in handling information related to people. Therefore, a SOC 2 examination that includes the trust services privacy category may encompass the service organization's specific processes that address the following, as applicable:

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

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.

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. Ordinarily, a type 2 report would 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.

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. Although management can delegate responsibility for these functions, management retains responsibility for the achievement of the service organization's service commitments and system requirements. When controls at 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 entity that owns the service organization.

[22] 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.

[23] 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).

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.

If the service organization's controls alone provide reasonable assurance that its service commitments and system requirements are achieved, or if the service organization's monitoring of the vendor's services and controls is sufficient to provide reasonable assurance that its service commitments and system requirements are achieved, the vendor's controls over its services are not likely to be relevant to the SOC 2 examination.

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:

- ABC Vendor is responsible for performing quarterly maintenance on the service organization's backup power system; service organization personnel participate in post-maintenance testing used to verify the backup power system is working as intended, which serves as a primary control. In this instance, ABC Vendor's controls are not necessary for the service organization to achieve its service commitments and system requirements based on the applicable trust services criteria for availability; therefore, ABC Vendor would not be considered a subservice organization.
- XYZ Vendor is responsible for monitoring service capacity and usage and for projecting future capacity demands based on historical trends. Without additional controls at the service organization, controls at the vendor are necessary for the service organization to achieve its service commitments and system requirements related to availability based on the applicable trust services criteria. Therefore, XYZ Vendor would be considered a subservice organization. However, if the service organization were to independently perform high-level capacity monitoring activities and review the future capacity demands projected by XYZ Vendor for appropriateness, XYZ Vendor might not be considered a subservice organization because the vendor's controls may not be necessary for the service organization to achieve its service commitments and system requirements based on the applicable trust services criteria. Management would need to determine, and the service auditor would need to agree, whether the review controls were precise enough that the vendor controls would not be necessary.
- A service organization outsources its application development testing to DEF Vendor and contractually specifies that certain controls be executed by DEF Vendor. The service organization designates a service organization employee to oversee the outsourced services, and that employee compares DEF Vendor's test plans, test scripts, and test data to the service organization's application change requests and detailed design documents. The designated service organization employee also reviews the results of testing performed by DEF Vendor before approving changes to the application and submitting them to the service organization for user acceptance testing. In this instance, even though the controls expected to be performed by DEF Vendor are stipulated in the contract, management concludes and the service auditor concurs that the controls at DEF Vendor are not necessary for the service organization to assert that its controls provide reasonable assurance that the service organization's availability commitments were achieved based on the applicable trust services criteria. Because the controls are not necessary, DEF Vendor would not be considered a subservice organization.

- A service organization purchases from JKL Vendor a tool to monitor and report on the status of configuration settings that affect the operation of control activities. JKL Vendor also provides services around the use of that tool through a SaaS model. In this situation, management has effectively outsourced monitoring of the configuration settings to JKL Vendor. Because management considers this function and related controls necessary to the achievement of the service organization's service commitments and system requirements, JKL Vendor would be considered a subservice organization.

Management's Use of Specialists

Increasingly, service organizations are using external specialists (management's specialists[24]) to leverage knowledge, technologies, experience, and expertise not resident within the service organization. If information produced by the management's specialist is used by the service auditor, the service auditor may need to perform further procedures to determine if such information is sufficiently reliable for the service auditor's purposes. Such management's specialists may include the following:

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

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

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

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

If the management's specialist is a subservice organization, the service organization's description of its system would include the information set forth in description criterion DC7 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, service organization management is responsible for determining whether to use the carve-out or inclusive method when addressing the subservice organization in the description of the system. 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:

[24] The term *management's specialist*, as used in this document, is defined as an individual or organization possessing expertise in a field other than accounting or attestation, whose work in that field is used by the service organization to assist the service organization in preparing the description or enhancing the effectiveness of controls.

- *Carve-out method*. Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system used to provide the services to the service organization are excluded from the description of the service organization's system and from the scope of the examination. However, the description identifies:
  - the nature of the services performed by the subservice organization;
  - the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and
  - the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.
- *Inclusive method*. Method of addressing the services provided by a subservice organization in which the description of the service organization's system includes a description of
  - the nature of the service provided by the subservice organization;
  - the components of the subservice organization's system used to provide services to the service organization, including the subservice organization's controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and
  - the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

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

When a service organization uses multiple subservice organizations, management may prepare the 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 would not be appropriate in situations in which the service auditor is not independent of both the service organization and the subservice organization because they are both responsible parties under this method.

The following are examples of circumstances in which the use of the carve-out method may be the most practical approach:

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

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

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

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

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, the suitability of the design of controls, and, in a type 2 examination, the operating effectiveness of the subservice organization's controls (including written representations from management of the subservice organization). If subservice organization management will not provide a written assertion and appropriate written representations, service organization management will be unable to use the inclusive method but may be able to use the carve-out method.

Identifying Complementary Subservice Organization Controls

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

Examples of CSOCs include the following:

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

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

Identifying Complementary User Entity Controls and User Entity Responsibilities

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

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

In most circumstances, a service organization's controls alone are sufficient to enable the achievement of its service commitments or system requirements. This is because, when making its service commitments, management only makes commitments that it is able to control. Similarly, system requirements are generally derived only from those commitments that are the service organization's responsibility. Therefore, management typically does not identify CUECs to be implemented by user entities.

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

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

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

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

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

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

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

- Access to the data center requires a documented access request form and manager approval prior to access being provisioned.
- A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.
- Access to the data center is reviewed quarterly by management.
- Persons are identified and authenticated through the badging access system prior to accessing the data center.
- In addition to the CUECs, the subservice organization may also identify user entity responsibilities that should be considered by the service organization to effectively use the subservice organization's system but that do not affect the subservice organization's ability to achieve its commitments to the service organization. Such activities may also be described in user documentation published by the subservice organization or in the agreement between the service organization and subservice organization.

Agreeing on the Terms of the Engagement

Service organization management and the service auditor should 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, such as an engagement letter, reduces the risk that either the service auditor or service organization management may misinterpret the needs or expectations of the other party. For example, it reduces the risk that management may rely on the service auditor to protect the service organization against certain risks or to perform certain management functions. For that reason, service organization management acknowledges these responsibilities in an engagement letter or other suitable form of written communication. If management refuses to provide the service auditor with an engagement letter, this may cause the service auditor to question whether a mutual understanding regarding the terms of the engagement has been reached and, in turn, may affect the service auditor's decision about whether to accept or continue the engagement.

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 AICPA

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

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

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

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

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. When 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.

Changes in Terms of the Examination

After the engagement agreement is executed but prior to the completion of the engagement, management may wish 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, professional standards will not allow the service auditor to 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

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

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
- Having a reasonable basis for its assertion
- 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
- If the service auditor plans to use internal auditors to provide direct assistance, providing the service auditor with written acknowledgment that internal auditors providing direct assistance to the service auditor will be allowed to follow the service auditor's instructions and that the service organization will not intervene in the work the internal auditors perform for the service auditor
- Providing the service auditor with the following:
  - Access to all information, such as records, documentation, service-level agreements, and internal audit or other reports, that management is aware of and that is relevant to the engagement
  - Access to additional information that the service auditor may request from management for purposes of the engagement
  - Unrestricted access to personnel within the service organization from whom the service auditor determines it is necessary to obtain evidence relevant to the SOC 2 examination

- Disclosing to the service auditor the following:
  - Incidents of noncompliance with laws and regulations, fraud, or uncorrected misstatements that are clearly not trivial and that may affect one or more user entities and whether such incidents have been communicated appropriately to affected user entities
  - Knowledge of any actual, suspected, or alleged fraud or noncompliance with laws and regulations affecting the description, suitability of design of controls, or, in a type 2 examination, operating effectiveness of controls
  - All deficiencies in the design of controls of which management is aware
  - All instances in which controls have not operated as described
  - All identified system incidents that were the result of controls that were not suitably designed or operating effectively or resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements as of the date of the description (for a type 1 examination) or during the period of time covered by the description (for a type 2 examination)

Management acknowledges these responsibilities in an engagement letter or other suitable form of written communication.

Preparing the Description of the Service Organization's System in Accordance With the Description Criteria

The description of the service organization's system presented in accordance with the description criteria is designed to enable user entities, business partners, and other intended users of the SOC 2 report (known collectively as *report users*) to understand the service organization's system, including the processing and flow of data and information through and from the system, and other information that may be useful when assessing the risks arising from interactions with the service organization's system, particularly system controls that service organization management has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the applica-ble 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, and 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. Service organization management may organize the description in a variety of different ways, provided that disclosures called for by the description criteria are included. For example, the description may be organized by components of internal control (the control environment, risk assessment process, control activities, monitoring activities, and information and communications). It may also be organized by components of the system (infrastructure, software, people, data, and processes and procedures). Management may use other logical groupings of information in organizing its system description including the use of recognized industry frameworks or standards based on management's objectives. For instance, the system description may be organized by control families or control objectives listed in a process or control framework.

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

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

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

When evaluating whether the description is presented in accordance with the description criteria, service organization management may consider the characteristics presented in table 1-3.

Table 1-3

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

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

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

Determining whether the description of a service organization's system presents a system that was implemented also involves evaluating whether each control stated in the description has been implemented.

When deciding how best to present controls, service organization management may select the format that best meets its objectives, the needs of its users, and its users' likely frame of reference; it may also consider the risks that use of a particular format may be misleading to users. Common formats for presenting controls in a SOC 2 report are included in the following examples:

Example 1:

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

Under this format, a control is often listed multiple times when it addresses more than one trust services criterion. Management is responsible for disclosing the controls; the service auditor is responsible for disclosing the description of tests performed and the results of such tests.

Example 2:

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

Example 3:

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

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.

Because the description presents primarily nonfinancial information, most descriptions are presented in narrative form. Thus, materiality considerations are mainly qualitative in nature and center around whether there is a substantial likelihood that misstatements, or omissions, in the information disclosed would, individually or in the aggregate, influence the judgments made by intended users of the SOC 2 report.

When evaluating the materiality of a description misstatement, the following qualitative factors may be considered:

- The interaction between, and relative importance of, individual disclosures within the description.
- The wording used to make the required disclosures. For example, the wording chosen does not omit or distort the disclosures presented.
- Whether the characteristics of the presentation are appropriate, given that the description criteria allow for variations in presentation.
- The extent to which identified deficiencies in the suitability of design or the operating effectiveness of controls contradict the disclosures about controls included in the description.
- The effect of the misstatement or potential misstatement on the description as a whole.
- The seriousness of the consequences of the misstatement to noncompliance with laws or regulations.

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. However, it does not describe the types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (CSOCs). Because understanding how the subservice organization's processes and controls may affect the achievement of the service organization's service commitments and system requirements is likely to be important to report users, a description misstatement in such information would be considered material to the description of the service organization's system.
- *Example 2.* Example 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 likelihood of 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 relevant to report users because controls over the encryption of the tapes prevent unauthorized access to the information and compensate for the omission of controls over physical access to the facility. Therefore, the omission of that information from the description would not be considered material.
- *Example 3.* Example Service Organization provides business users with a web-based customer relationship management system. Management has identified certain deficiencies in the design of controls that protect customer data from unauthorized access. Because business users of the system are interested in maintaining the confidentiality of their customer relationships, deficiencies in such controls are likely to be considered significant to such users. Therefore, the omission of such deficiencies from the description would be considered material.
- *Example 4.* Management of Example Service Organization makes certain claims within the description about the service organization's compliance with published privacy practices. The service organization also shares the email addresses of certain user entity customers with a related party for use when marketing the related party's products. Because this constitutes an intentional violation of published privacy practices and involves a related-party relationship, the omission of the identified control deficiency is a material misstatement in the description.

Performance of a Risk Assessment and Having a Reasonable Basis for Management's Assertions

Service organization management is responsible for having a reasonable basis for its assertion about the description, the suitability of design of controls and, in a type 2 engagement, operating effectiveness of controls stated therein. Furthermore, because management's assertion generally addresses the suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls over a period of time, management's basis for its assertion covers the same time frame. Having a reasonable basis necessitates the performance of risk assessment, the implementation of effective processes and controls to mitigate identified risks, and the performance of controls and other activities to monitor the effectiveness of such controls. Also inherent is the assumption that service organization management possesses the necessary skills and competence to perform these functions. Such skills and competence are necessary to enable management to oversee the work of vendors, management's specialists, and other third parties who assist management with the effective operation of internal control. (The procedures performed by the service auditor during a 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 third parties such as user entities, business partners, subservice organizations, vendors, and others who have access to the service organization's system, or otherwise transmit information back and forth between, or on behalf of, the service organization. Therefore, it is important for service organization management to assess the risks arising from interactions with those parties, particularly when they operate controls necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

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

- Testing controls at the third party by members of the service organization's internal audit function
- Reviewing and reconciling output reports

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

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 writeups, 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 a 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.

Designing and Implementing Effective Controls

As previously discussed, the risk assessment enables management to identify and assess the risks that threaten the achievement of the service organization's service commitments and system requirements; such assessments are necessary for management to implement effective controls to mitigate those risks.

Service organization management is responsible for designing, implementing, and monitoring controls that provide reasonable assurance that the service organization's service commitments and system requirements were achieved. They are also responsible for modifying the controls as necessary based on new and evolving risks, evaluating the linkage between the controls and the evolving risks and threats to the achievement of the service commitments and system requirements.

Suitably designed controls, if implemented and operating effectively, provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria. Suitably designed controls operate as designed by persons who have the necessary authority and competence to perform the controls. Management ensures that controls are operating as designed by performing monitoring activities.

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

Examples of monitoring activities that service organization management may perform, which also support management's basis for its assertion, include the following:

- Reviewing results of control evaluations performed by the internal audit function
- Periodic evaluation of control effectiveness through self-assessment or quality assurance programs
- Ongoing monitoring or direct management oversight, such as daily meetings with control executers
- A combination of the various assessment techniques

Service organization management generally documents the performance of monitoring activities.

Providing the Service Auditor With a Written Assertion[25]

In a SOC 2 examination, service organization management has to provide the service auditor with a written assertion that 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.

[25] 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.

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 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.

AICPA® & CIMA®

Together as the Association of International
Certified Professional Accountants

P: 888.777.7077 | F: 800.362.5066 | W: aicpa-cima.com

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.