Information for service organization management
This document is nonauthoritative and is included 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:** The contents of this publication do not necessarily reflect the position or opinion of the American Institute of CPAs, its divisions and its committees. This publication is designed to provide accurate and authoritative information on the subject covered. It is distributed with the understanding that the authors are not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

For more information about the procedure for requesting permission to make copies of any part of this work, please email copyright@aicpa.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, 220 Leigh Farm Road, Durham, NC 27707–8110.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Introduction and background</td>
</tr>
<tr>
<td>4</td>
<td>Intended users of a SOC 2&lt;sup&gt;®&lt;/sup&gt; report</td>
</tr>
<tr>
<td>6</td>
<td>Overview of a SOC 2&lt;sup&gt;®&lt;/sup&gt; examination</td>
</tr>
<tr>
<td>7</td>
<td>Contents of the SOC 2&lt;sup&gt;®&lt;/sup&gt; report</td>
</tr>
<tr>
<td>8</td>
<td>Difference between privacy and confidentiality</td>
</tr>
<tr>
<td>9</td>
<td>Description criteria</td>
</tr>
<tr>
<td>10</td>
<td>Trust services criteria</td>
</tr>
<tr>
<td>11</td>
<td>Categories of criteria</td>
</tr>
<tr>
<td>13</td>
<td>The service organization’s service commitments and system requirements</td>
</tr>
<tr>
<td>15</td>
<td>SOC 2&lt;sup&gt;®&lt;/sup&gt; examination that addresses additional subject matters and additional criteria</td>
</tr>
<tr>
<td>16</td>
<td>SOC 3&lt;sup&gt;®&lt;/sup&gt; examination</td>
</tr>
<tr>
<td>17</td>
<td>Other types of SOC examinations: SOC suite of services</td>
</tr>
<tr>
<td>18</td>
<td>SOC for cybersecurity</td>
</tr>
<tr>
<td>19</td>
<td>Management responsibilities in a SOC 2&lt;sup&gt;®&lt;/sup&gt; Examination prior to engaging the service auditor</td>
</tr>
<tr>
<td>20</td>
<td>Defining the scope of the examination</td>
</tr>
<tr>
<td>22</td>
<td>Selecting the trust services category or categories to be addressed by the examination</td>
</tr>
<tr>
<td>24</td>
<td>Determining whether to use the inclusive or carve-out method</td>
</tr>
<tr>
<td>26</td>
<td>Identifying complementary subservice organization controls</td>
</tr>
<tr>
<td>27</td>
<td>Identifying complementary user entity controls and user entity responsibilities</td>
</tr>
<tr>
<td>28</td>
<td>Identifying controls that a subservice organization expects the service organization to implement</td>
</tr>
<tr>
<td>30</td>
<td>Management responsibilities during the examination</td>
</tr>
<tr>
<td>31</td>
<td>Preparing the description of the service organization’s system in accordance with the description criteria</td>
</tr>
<tr>
<td>32</td>
<td>Materiality considerations when preparing the description in accordance with the description criteria</td>
</tr>
<tr>
<td>33</td>
<td>Having a reasonable basis for the assertion</td>
</tr>
<tr>
<td>34</td>
<td>Providing the service auditor with a written assertion</td>
</tr>
<tr>
<td>35</td>
<td>Modifying management’s assertion</td>
</tr>
<tr>
<td>36</td>
<td>Providing the service auditor with written representations</td>
</tr>
<tr>
<td>36</td>
<td>Endnotes</td>
</tr>
</tbody>
</table>
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) can 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 the service organization implements to protect the business partners’ intellectual property.

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

• Customer support — Providing customers of user entities with online or telephonic post-sales support and service management — examples of these services are warranty inquiries and investigating and responding to customer complaints

• Health care claims management and processing — Providing medical providers, employers, third-party administrators and insured parties of employers with systems that enable medical records and related health insurance claims to be processed accurately, securely and confidentially

• Enterprise IT outsourcing services — Managing, operating and maintaining user entities’ IT data centers, infrastructure and application systems and related functions that support IT activities, such as network, production, security, change management, hardware and environmental control activities

• Managed security — Managing access to networks and computing systems for user entities (for example, granting access to a system and preventing, or detecting and mitigating, system intrusion)

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

Although these relationships may increase revenues, expand market opportunities and reduce costs for the user entities and business partners, they also result in additional risks arising from interactions with the service organization and its system. Accordingly, the management of those user entities and business partners are responsible for identifying, evaluating and addressing those additional risks as part of their risk assessment. In addition, although management can delegate responsibility for specific tasks or functions to a service organization, management remains accountable for those tasks to boards of directors, shareholders, regulators, customers and other affected parties. As a result, management is responsible for establishing effective internal control over interactions between the service organizations and their systems.
To assess and address the risks associated with a service organization, its services and the system used to provide the services, user entities and business partners usually need information about the design, operation and effectiveness of controls within the system. To support their risk assessments, user entities and business partners may request a SOC 2® report from the service organization. A SOC 2® report is the result of an examination of whether: (a) the description of the service organization's system presents the system that was designed and implemented in accordance with the description criteria, (b) the suitability of the design of controls would provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the criteria, if those controls operated effectively, and (c) in a type 2 examination, the controls stated in the description operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the criteria relevant to the security, availability or processing integrity of the service organization's system (security, availability and 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). This examination is referred to as a SOC 2® examination.

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

- A type 1 examination is an examination of whether:
  - a service organization's description presents the system that was designed and implemented as of a point in time in accordance with the description criteria and
  - controls were suitably designed as of a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

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

  A report on such an examination is referred to as a type 2 report.

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

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

A SOC 2® report is intended for use by those who have sufficient knowledge and understanding of the service organization, the services it provides and the system used to provide those services, among other matters. Without such knowledge, users are likely to misunderstand the content of the SOC 2® report, the assertions made by management and the service auditor’s opinion, all of which are included in the report. For that reason, management and the service auditor should agree on the intended users of the report (referred to as specified parties). The expected knowledge of specified parties ordinarily includes:

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

Specified parties that are likely to possess sufficient knowledge to understand a SOC 2® report may include service organization personnel, user entities of the system throughout some or all the period, business partners subject to risks arising from interactions with the system, practitioners providing services to user entities and business partners, and regulators who have sufficient knowledge and understanding of such matters.

Other parties may also have the requisite knowledge and understanding. For example, prospective user entities or business partners, who intend to use the information contained in the SOC 2® report as part of their vendor selection process or to comply with regulatory
requirements for vendor acceptance, may have gained such knowledge while performing due diligence. (If prospective users lack such knowledge and understanding, management may instead engage a service auditor to provide a SOC 3® report, as discussed later.)

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

In some situations, service organization management may wish to distribute a report on the service organization’s controls relevant to security, availability, confidentiality, processing integrity or privacy to users who lack the knowledge and understanding required to understand the SOC 2® report. In that case, management may engage a service auditor to examine and express an opinion on the effectiveness of controls within a service organization system in a SOC 3® examination. A SOC 3® report is ordinarily appropriate for general users. (See the section titled “SOC 3® examination.”)
Overview of a SOC 2® examination

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

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

In a SOC 2® examination, service organization management is the responsible party. However, in certain situations there may be other responsible parties. As the responsible party, service organization management prepares the description of the service organization’s system that is included in the SOC 2® report. In addition, the service auditor is required by the attestation standards to request a written assertion from management. Management’s written assertion addresses whether (a) the description of the service organization’s system is presented in accordance with the description criteria, (b) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria, and (c) in a type 2 examination, those controls were operating effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria.

The service auditor designs and performs procedures to obtain sufficient appropriate evidence about whether the description presents the system that was designed and implemented in accordance with the description criteria and whether (a) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria and, (b) in a type 2 examination, those controls were operating effectively to provide reasonable assurance that the service organization’s 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® report

A SOC 2® examination results in the issuance of a SOC 2® report. As shown in table 1-1, the SOC 2® report includes three key components.

<table>
<thead>
<tr>
<th>Table 1-1&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contents of a SOC 2® report</strong></td>
</tr>
<tr>
<td><strong>Type 1 report</strong></td>
</tr>
<tr>
<td>1. Description of the system as of a point in time in accordance with the description criteria</td>
</tr>
<tr>
<td>2. Management assertion that addresses whether:</td>
</tr>
<tr>
<td>a. the description of the service organization's system as of a point in time is presented in accordance with the description criteria and</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>3. The service auditor's opinion about whether:</td>
</tr>
<tr>
<td>a. the description of the service organization's system as of a point in time is presented in accordance with the description criteria and</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>4. Description of the service auditor's tests of controls and results thereof</td>
</tr>
<tr>
<td>2. Management assertion that addresses whether:</td>
</tr>
<tr>
<td>a. the description of the service organization's system throughout a period is presented in accordance with the description criteria,</td>
</tr>
<tr>
<td>b. the controls stated in the description were suitably designed throughout a period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and</td>
</tr>
<tr>
<td>c. the controls stated in the description operated effectively throughout a period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria</td>
</tr>
<tr>
<td>3. The service auditor's opinion about whether:</td>
</tr>
<tr>
<td>a. the description of the service organization's system throughout a period is presented in accordance with the description criteria,</td>
</tr>
<tr>
<td>b. the controls stated in the description were suitably designed throughout a period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and</td>
</tr>
<tr>
<td>c. the controls stated in the description operated effectively throughout a period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria</td>
</tr>
</tbody>
</table>

<sup>a</sup> Table 1-1 from the original document.
Difference between privacy and confidentiality

Some individuals consider effective privacy practices to be the same as effective practices over confidential information. Privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. Therefore, a SOC 2® examination that includes the trust services privacy criteria encompasses the service organization’s specific processes that address each of the following, as applicable:

• Notice of the service organization’s privacy commitments and practices
• Data subjects’ choices regarding the use and disclosure of their personal information
• Data subjects’ rights to access their personal information for review and update
• An inquiry, complaint and dispute resolution process

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

Criteria for a SOC 2® examination

The following 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, 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, 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 an examination.
Description criteria

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

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

The description criteria in DC section 200 were promulgated by the Assurance Services Executive Committee (ASEC), which is designated by the Council of the AICPA under the AICPA Code of Professional Conduct to issue measurement criteria. Therefore, such criteria are considered suitable for use in a SOC 2® examination. Because the AICPA publishes the description criteria and made it available to the public, they are considered available to report users. Therefore, the description criteria are both suitable and available for use in a SOC 2® engagement.
Trust services criteria

The trust services criteria in TSP section 100 are used to evaluate the suitability of the design and operating effectiveness of controls related to one or more of the trust services categories (security, availability, processing integrity, confidentiality and privacy). The engaging party, typically service organization management, may choose to engage the service auditor to report on controls related to one or more of these categories.

Service organization management evaluates the suitability of the design and operating effectiveness of controls stated in the description to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to the trust services category or categories included within the scope of the examination. Such criteria are referred to as the applicable trust services criteria. For example, in a SOC 2® examination that addresses security, the trust services criteria relevant to security, which are the common criteria (CC1.1–CC9.2) presented in TSP section 100, would be the applicable trust services criteria.

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

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

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

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

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

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

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

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

d. Confidentiality — Information designated as confidential is protected to meet the entity’s objectives.

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

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

• criteria common to all five of the trust service categories (common criteria) and

• additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

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

Common criteria

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

a. Control environment (CC1 series)

b. Communication and information (CC2 series)

c. Risk assessment (CC3 series)

d. Monitoring activities (CC4 series)

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

Table 1–2 identifies the trust services criteria to be used when evaluating the design or operating effectiveness of controls for each of the trust services categories. As shown in that table, the common criteria constitute the complete set of criteria for the security category. For the categories of availability, processing integrity, confidentiality and privacy, a complete set of criteria consists of (a) the common criteria (labeled in the table in TSP section 100 as the CC series) and (b) the criteria applicable to the specific trust services category or categories addressed by the examination, which are labeled in the table in TSP section 100 as follows:

a. Availability (A series)

b. Processing integrity (PI series)

c. Confidentiality (C series)

d. Privacy (P series)

Because each system and the environment in which it operates are unique, the combination of risks that would prevent a service organization from achieving its service commitments and system requirements, and the controls necessary to address those risks, will be unique in each SOC 2® examination. Management needs to identify the specific risks that threaten the achievement of the service organization’s service commitments.
and system requirements and the controls necessary to provide reasonable assurance that the applicable trust services criteria are met, which would mitigate those risks.

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 the 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.

Table 1–2

Criteria for evaluating the design and operating effectiveness of controls

<table>
<thead>
<tr>
<th>Trust services category</th>
<th>Common criteria</th>
<th>Additional category-specific criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Processing integrity</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

16 This table can also be found in chapter 1 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.
The service organization’s service commitments and system requirements

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

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

- Specification of the algorithm used in a calculation
- The hours a system will be available
- Published password standards
- Encryption standards used to encrypt stored customer data

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

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

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

- Workforce member fingerprinting and background checks established in government banking regulations
- System edits that restrict the values accepted for system input, which are defined in application design documents
- Maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual
- Data definition and tagging standards, including any associated metadata requirements (for example, the Simple Object Access Protocol [SOAP]), established by industry groups or other bodies
• Business processing rules and standards established by regulators (for example, security requirements under the Health Insurance Portability and Accountability Act [HIPAA])

System requirements may result from the service organization’s commitments relating to one or more of the trust services categories (for example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration).

Service organization management is responsible for achieving its service commitments and system requirements. It is also responsible for stating in the description the service organization’s principal service commitments and system requirements with sufficient clarity to enable report users to understand how the system operates and how management and the service auditor evaluated the suitability of the design of controls and, in a type 2 examination, the operating effectiveness of controls. Because of the importance of the service commitments and system requirements to the SOC 2® examination, the principal service commitments and system requirements disclosed by management should be appropriate for the engagement. Chapter 2 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy 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.
Management may engage the service auditor to examine and report on the subject matter in addition to the description of the service organization’s system in accordance with the description criteria and the suitability of the design and operating effectiveness of controls based on the applicable trust services criteria. In that case, the service auditor would also examine and report on whether the additional subject matter is presented in accordance with the additional suitable criteria used to evaluate it. Table 1-3 provides examples of additional subject matters and additional criteria that may be used to evaluate them.

### Table 1-3

<table>
<thead>
<tr>
<th>What additional information might be included in the SOC 2® report?</th>
<th>What are the subject matters?</th>
<th>What are suitable criteria relevant to the subject matters?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information on the physical characteristics of a service organization’s facilities (for example, square footage)</td>
<td>A detailed description of certain physical characteristics of a service organization’s facilities that includes items such as the square footage of the facilities</td>
<td>Criteria to evaluate the presentation of the description of the physical characteristics of the facilities</td>
</tr>
<tr>
<td>Information about historical data regarding the availability of computing resources at a service organization</td>
<td>Historical data related to the availability of computing resources</td>
<td>Criteria to evaluate the completeness and accuracy of the historical data</td>
</tr>
<tr>
<td>Information about how controls at a service organization help meet the organization’s responsibilities related to the security requirements of HIPAA</td>
<td>Compliance with the HIPAA security requirements</td>
<td>Security requirements set forth in the HIPAA Administrative Simplification (Code of Federal Regulations, Title 45, Sections 164.308–316)</td>
</tr>
<tr>
<td>Information about how controls at a service organization address the Cloud Security Alliance’s Cloud Controls Matrix</td>
<td>Controls related to security at a cloud service provider</td>
<td>Criteria established by the Cloud Security Alliance’s Cloud Controls Matrix relevant to the security of a system</td>
</tr>
</tbody>
</table>

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

- An appropriate description of the subject matter
- A description of the criteria identified by management used to measure and present the subject matter
- If the criteria are related to controls, a description of the controls intended to meet the control-related criteria
- An assertion by management regarding the additional subject matter or criteria
SOC 3® examination

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

In this situation, a SOC 3® report, which is a general use report, may be more appropriate. Because the procedures performed in a SOC 2® examination are substantially the same as those performed in a SOC 3® examination, the service organization may ask the service auditor to issue two reports at the end of the examination: a SOC 2® report to meet the governance needs of its existing customers and a SOC 3® report to meet more general user needs.

In a SOC 3® examination, service organization management prepares, and includes in the SOC 3® report, a written assertion about whether the controls within the system were effective 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. Regarding 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.

Other types of SOC examinations:
SOC suite of services

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

1. SOC 1® — SOC for Service Organizations: ICFR
2. SOC 2® — SOC for Service Organizations: Trust Services Criteria
3. SOC 3® — SOC for Service Organizations: Trust Services Criteria for General Use Report
4. SOC for Cybersecurity
SOC 1® — SOC for Service Organizations: ICFR

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

Service organizations frequently receive requests from user entities for these reports because the auditors of the user entities’ financial statements (user auditors) need them to obtain information about controls at the service organization that may affect assertions in the user entities’ financial statements. A SOC 1® report is intended solely for the information and use of existing user entities (for example, existing customers of the service organization), their financial statement auditors, and management of the service organization. The AICPA Guide Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting (SOC 1®) contains application guidance for service auditors.
SOC for cybersecurity

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

For those reasons, entities have begun requesting practitioners to examine and report on a description of the entity’s cybersecurity risk management program and the effectiveness of controls within the program. This examination is known as a cybersecurity risk management examination; the related report is known as a cybersecurity risk management examination report. The performance and reporting requirements for such an examination are found in AT-C section 105 and AT-C section 205. The AICPA Guide Reporting on an Entity’s Cybersecurity Risk Management Program and Controls contains interpretive application guidance for practitioners performing these engagements.

The cybersecurity risk management examination report includes three key components: (a) the description of the entity’s cybersecurity risk management program, (b) management’s assertion about whether the description is presented in accordance with the description criteria and whether the controls within the cybersecurity risk management program were effective to achieve the entity’s cybersecurity objectives based on the control criteria, and (c) the practitioner’s opinion about whether the description is presented in accordance with the description criteria and whether the controls within the cybersecurity risk management program were effective to achieve the entity’s cybersecurity objectives based on the control criteria.

In the cybersecurity risk management examination, management selects the criteria to be used to prepare the description of the entity’s cybersecurity risk management program (description criteria) and the criteria to be used to evaluate the effectiveness of controls within that program (control criteria). The AICPA Guide Reporting on an Entity’s Cybersecurity Risk Management Program and Controls contains description criteria and trust services criteria for security, availability and confidentiality, which may be used in the cybersecurity risk management examination.

Because the practitioner’s report is designed to be included in the cybersecurity risk management examination report, which is intended for general distribution, the practitioner’s report is appropriate for general use. Nevertheless, practitioners may decide to restrict the use of the report to specified users.
Management responsibilities in a SOC 2® examination prior to engaging the service auditor

Prior to engaging a service auditor to perform a SOC 2® examination, service organization management is responsible for making a variety of decisions that affect the nature, timing and extent of procedures to be performed in a SOC 2® examination, including the following:

• Defining the scope of the examination, which includes the following:
  — Identifying the services provided to user entities, which will establish the subject matter of the examination
  — Identifying the system used to provide those services
  — Identifying the risks from business partners providing intellectual property or services to the service organization related to the system
  — Selecting the trust services category or categories to be included within the scope of the examination
  — Determining the type (type 1 or type 2) of SOC 2® examination to be performed
  — Determining the period to be covered by the examination or, in the case of a type 1 report, the specified “as of” date
  — If services are provided to the service organization by other entities, evaluating the effect of those services on the service organization’s achievement of its service commitments and system requirements and concluding whether those other entities are subservice organizations
  — Determining whether subservice organizations, if any, are to be addressed in the report using the inclusive method or the carve-out method
  — If a subservice organization is to be presented using the inclusive method, obtaining agreement from subservice organization management to participate in the examination
• Specifying the principal service commitments made to user entities and the system requirements needed to operate the system
• Specifying the principal system requirements related to commitments made to business partners
• Identifying and analyzing risks that could prevent the service organization from achieving its service commitments and system requirements
• Designing, implementing, operating, monitoring and documenting controls that are suitably designed and, in a type 2 examination, operating effectively to provide reasonable assurance of achieving the service organization’s service commitments and system requirements based on the applicable trust services criteria

To increase the likelihood that the description and service auditor’s report will be useful to report users, service organization management may discuss some or these matters with intended users prior to engaging the service auditor.
Defining the scope of the examination

The scope of a SOC 2® engagement is defined by the services that the service organization provides to user entities. Services involve the performance of a function on behalf of the user entities. Services may be provided in conjunction with the provision of goods either through lease or sale and may be difficult to distinguish from the lease or sale. For example, maintenance services may be provided in conjunction with the sale of equipment, whereas warranty work performed on the same equipment may not be considered a service but rather a part of the purchase of the equipment. Services may also be dependent on the provision of equipment from the service organization to the user entity. For example, the provision of security monitoring services may require user entities to install the service organization’s proprietary software on computer servers in the user entity’s network. The services addressed by a SOC 2® examination usually are common to many of its user entities and specified in written agreements between the service organization and the user entities.

Often, service organizations bundle multiple services together as incentives to user entities or to provide the individual services more efficiently and effectively. When the service organization wishes to include only a portion of commonly bundled services in a SOC 2® report, management should consider whether the portion of the services is an appropriate subject matter. Factors to consider include:

- Will the intended report users understand which services are included in the scope of the SOC 2® report and which are not? If there is a likelihood that report users will conclude that all services are covered in the scope of the examination when only a portion of the services are covered, report users may misunderstand the results of the examination.

When defining the services to be covered by the SOC 2® report, management may find it useful to consider how services are presented in agreements with user entities and how the services are described in service documentation. These agreements may also establish requirements for the service organization to have a SOC 2® engagement. In such instances, the services to be covered may be explicitly stated in the agreement.

Identifying the system

In the SOC 2® examination, a system is defined as the following:

The infrastructure, software, procedures and data that are designed, implemented and operated by people to achieve one or more of the organization’s specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

The bolded 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 the system uses, such as transaction streams, files, databases, tables and other output used or processed by the system

- Procedures — The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed and delivered, and reports and other information prepared

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

In 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.

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

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.
Selecting the trust services category or categories to be addressed by the examination

In a SOC 2® engagement, the trust services criteria are used to evaluate the suitability of the design and operating effectiveness of controls relevant to one or more of the trust services categories of security, availability, processing integrity, confidentiality and privacy. These categories relate to areas of concern for report users; however, not all services are subject to the same level of concern for each category. When determining the scope of the SOC 2® examination, management determines which categories are likely to be of interest to report users and includes them within the scope of the examination. For example, security and availability may be of concern to user entities of a service organization providing IT infrastructure collocation services; however, processing integrity is unlikely to be of concern to them. Written agreements may provide information on which category or categories should be included within the scope of the SOC 2® examination.

Period the examination covers

Service organization management is responsible for determining the time frame the description of the service organization’s system will cover, 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. Regardless of the time frame selected, the SOC 2® examination contemplates that the time frame is the same for both the description and management’s assertion.

For SOC 1® examinations, user entities usually have very explicit needs with respect to the period covered by the examination. Those needs usually do not exist for a SOC 2® report. However, a type 2 report should cover a period that is sufficient for the service auditor to obtain sufficient appropriate evidence about the suitability of design and operating effectiveness of the controls. Beyond that consideration, the frequency and the period covered by a SOC 2® report is a business decision of management. Many service organizations use the same period for their SOC 1® and SOC 2® examinations because that is often the most efficient approach.

Identifying subservice organizations

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

A vendor is considered a subservice organization only if the following apply:

- The services the vendor provides are likely to be relevant to report users’ understanding of the services organization’s system as it relates to the applicable trust services criteria.
- Controls at the vendor are necessary, in combination with the service organization’s controls, to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria.
If the service organization’s controls alone achieve its service commitments and system requirements, or if the service organization’s monitoring of the vendor’s services and controls is sufficient to achieve its service commitments and system requirements, the vendor provides are not likely to be relevant to the SOC 2® examination.

Service organization management is responsible for determining whether it uses a subservice organization. Making that determination is not always easy, as illustrated by the following examples:

• A vendor that is responsible for performing quarterly maintenance on a service organization’s backup power system in an examination that addresses availability — This vendor would not be considered a subservice organization if the service organization implements its own controls over the vendor’s services and vendor controls over its maintenance activities are not necessary, in combination with the service organization’s controls, to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria for availability.

• A vendor that provides data center hosting services — If that vendor is responsible for monitoring server capacity and usage and for projecting future capacity demands based on historical trends, controls at the vendor may be needed for the service organization to achieve its availability commitments based on the applicable trust services criteria for availability. On the other hand, controls at the vendor may not be necessary if the service organization independently performs high-level capacity monitoring activities and reviews the future capacity demands projected by the vendor for appropriateness.

In some instances, a service organization may stipulate in its contract with the vendor that the vendor perform certain controls that the service organization believes are necessary to address the risks related to the vendor’s services. For example, a service organization may outsource its application development testing to a vendor and contractually specify that the vendor executes certain controls. The service organization designates a service organization employee to oversee the outsourced services, and that employee compares the vendor’s test plans, test scripts and test data to the service organization’s application change requests and detailed design documents. The designated service organization employee also reviews the results of testing performed by the vendor before changes to the application are approved by the vendor and submitted to the service organization for user acceptance testing. In this instance, the controls at the vendor may not be necessary for the service organization to assert that its controls provide reasonable assurance that the service organization’s availability commitments were achieved based on the applicable trust services criteria.
Determining whether to use the inclusive or carve-out method

If the service organization uses a subservice organization, management is responsible for determining whether to carve out or include the subservice organization’s controls within the scope of the examination. For that reason, it is important that management understand the differences between the two methods and the implications that arise from the choice of one method over the other. The two methods are defined as follows:

- **Carve-out method** — Method of addressing the services a subservice organization provides in which the components of the subservice organization’s system used to provide the services to the service organization are excluded from the description of the service organization’s system and from the scope of the examination. However, the description identifies (1) the nature of the services performed by the subservice organization; (2) the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved; and (3) the controls at the service organization used to monitor the effectiveness of the subservice organization’s controls.

- **Inclusive method** — Method of addressing the services a subservice organization provides in which the description of the service organization’s system includes a description of (a) the nature of the service provided by the subservice organization and (b) the components of the subservice organization’s system used to provide services to the service organization, including the subservice organization’s controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved. (When using the inclusive method, controls at the subservice organization are subject to the service auditor’s examination procedures. Because the subservice organization’s system components are included in the description, those components are included in the scope of the examination.)

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

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

- The services the subservice organization provides are extensive.
- A type 1 or type 2 report that meets the needs of report users is not available from the subservice organization.
- Information about the subservice organization is not readily available from other sources.

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

a. The challenges entailed in implementing the inclusive method, including the extensive planning and communication required among the service auditor, the service organization, and the subservice organization, are sufficiently onerous that it is not practical to use the inclusive method.

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

c. A type 1 or type 2 service auditor’s report on the subservice organization, which meets the needs of report users, is available.
d. The service organization is unable to obtain 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, management would consider whether the use of the carve-out method may result in a description of the service organization's system that is so limited that it is unlikely to be useful to the intended users of the report. When making this determination, the following factors may be helpful:

• The significance of the portion of the system functions the subservice organization performs

• The complexity of the services and the types of controls that would be expected to be implemented by the subservice organization

• The extent to which the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria depends on controls at the subservice organization

• The number of applicable trust services criteria that would not be met if the types of controls expected to be implemented at the subservice organization were not implemented

• The ability of the intended users of the report to obtain sufficient appropriate evidence about the design and, in a type 2 examination, the operating effectiveness of 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 appropriately written representations, service organization management will be unable to use the inclusive method but may be able to use the carve-out method.

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

In a SOC 2 examination in which the service organization uses the services of a subservice organization, and management elects to use the inclusive method to present certain information about the services the subservice organization provided, subservice organization management is also responsible for many of the matters described previously as they relate to the subservice organization. Accordingly, prior to engaging the service auditor, management and the service auditor discuss whether it will be possible to obtain (a) an assertion from subservice organization management and (b) evidence that supports the service auditor's opinion on the subservice organization's description of its system and the suitability of the design and, in a type 2 examination, the operating effectiveness of the subservice organization's controls (including written representations from management of the subservice organization). If subservice organization management will not provide a written assertion and appropriately written representations, service organization management will be unable to use the inclusive method but may be able to use the carve-out method.
Identifying complementary subservice organization controls

As discussed earlier, a subservice organization exists when management identifies certain risks that it expects controls implemented by that subservice organization to address. When the carve-out method is used, and controls the subservice organization performs are necessary, in combination with the service organization’s controls, to provide reasonable assurance that one or more of the service organization’s service commitments and system requirements were achieved, such controls are referred to as **complementary subservice organization controls** (CSOCs).23

Examples of CSOCs include the following:

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

Service organization management is required to disclose in its description the types of CSOCs that the subservice organization is assumed to have implemented. In some cases, management may request the service auditor’s assistance when determining how to present the CSOCs in the description. For example, the service auditor can provide examples of CSOC disclosures made by others and can make recommendations to improve the presentation of the CSOCs in the description.
Identifying complementary user entity controls and user entity responsibilities

Usually, user entities must perform specific activities to benefit from the services of a service organization. Such activities may include specifying the configuration of services to be provided, submitting authorized input for processing, managing user entity employee access to data and reviewing the outputs of processing. These activities may be specified in agreements between the user entity and the service organization, user manuals and other communications. Most of these activities are needed for the user entity to derive value from the service and do not affect the ability of the service organization to achieve its service commitments and system requirements. These activities are referred to as user entity responsibilities. However, in some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the user entity performing certain activities in a defined manner. In these instances, the service organization expects the user entity to implement necessary controls and to perform them completely and accurately in a timely manner. Such controls are referred to as complementary user entity controls (CUECs).

A service organization’s controls are usually able to provide reasonable assurance that the service organization's service commitments or system requirements were achieved without the implementation of CUECs because the service organization restricts its service commitments and system requirements to those matters that are its responsibility and that it can reasonably perform. Consider, for example, trust services criterion CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. Trust services criterion CC6.2 limits the service organization's responsibilities because the criterion requires only that the system register a user (a user identified by the user entity as an authorized user) and issue system credentials to that user after the user entity supplies the service organization with a list of authorized users.

If the user entity supplies the service organization with a list of authorized users that inadvertently includes employees who should not have been included, the service organization has still met CC6.2. Because providing the service organization with a list of authorized users is necessary for the user entity to benefit from the services provided by the service organization, it is a user entity responsibility. However, because the service organization’s controls provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criterion without such information, identifying the authorized users and communicating that information to the service organization are not considered CUECs.

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

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

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

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

- Access control software and rule sets are used to restrict logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output and offline system components.

- Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.

- Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.

- Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software.

Agreeing on the terms of the engagement

The attestation standards require the service organization and the service auditor to agree on, and document in a written communication, such as an engagement letter, the terms of the engagement with the engaging party. A written agreement reduces the risk that either the service auditor or service organization management may misinterpret the needs or expectations of the other party. For example, it reduces the risk that management may rely on the service auditor to protect the service organization against certain risks or to perform certain management functions. For that reason, service organization management acknowledges these responsibilities in an engagement letter or another suitable form of written communication.

The engagement letter should include:

a. The objective and scope of the engagement

b. The responsibilities of the service auditor

c. A statement that the engagement will be conducted in accordance with attestation standards established by the American Institute of CPAs

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 after the engagement

If the service auditor plans to use internal auditors to provide direct assistance, prior to doing so, the service auditor will also request written acknowledgment from service organization management that internal auditors providing direct assistance will be allowed to follow the service auditor’s instructions and that management will not intervene in the work the internal auditor performs for the service auditor. If service organization management is the engaging party, it is likely that this matter will also be included in the engagement letter.

In addition to these matters, the service auditor may decide to include other matters in the engagement letter, such as the identification of the service organization’s service commitments and system requirements.
Management responsibilities during the examination

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

- Preparing a description of the service organization’s system, including the completeness, accuracy, and method of presentation of the description
- Providing a written assertion that accompanies the description of the service organization’s system, both of which will be provided to report users
- Identifying the risks that threaten the service organization’s achievement of its service commitments and system requirements stated in the description
- Providing the service auditor with written representations after the engagement
- Designing, implementing and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the service commitments and system requirements will be achieved based on the applicable trust services criteria
- Having a reasonable basis for its assertion
- If the service auditor plans to use internal auditors to provide direct assistance, providing the service auditor with written acknowledgment that internal auditors providing direct assistance to the service auditor will be allowed to follow the service auditor’s instructions and that the service organization will not intervene in the work the internal auditor performs for the service auditor
- Providing the service auditor with the following:
  - Access to additional information that the service auditor may request from management for the examination
  - Unrestricted access to personnel within the service organization from whom the service auditor determines it is necessary to obtain evidence relevant to the SOC 2® examination
  - Access to additional information that the service auditor may request from management for the examination
- Disclosing to the service auditor the following:
  - Incidents of noncompliance with laws and regulations, fraud or uncorrected misstatements that are clearly not trivial and that may affect one or more user entities and whether such incidents have been communicated appropriately to affected user entities
  - Knowledge of any actual, suspected, or alleged intentional acts that could adversely affect the presentation of the description of the service organization’s system, the suitability of design of its controls, or, in a type 2 examination, the operating effectiveness of controls
  - Any deficiencies in the design of controls of which it is aware
  - All instances in which controls have not operated as described
  - All identified system incidents that resulted in a significant impairment of the service organization’s achievement of its service commitments and system requirements as of the date of the description (for a type 1 examination) or during the period covered by the description (for a type 2 examination)
  - Any events after the period covered by the description of the service organization’s system, up to the date of the service auditor’s report, that could have a significant effect on management’s assertion
Preparing the description of the service organization’s system in accordance with the description criteria

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

Service organization management is responsible for preparing the description of the system that was designed and implemented in accordance with the description criteria in DC section 200. Generally, management prepares the description from documentation supporting the system of internal control and system operations, as well from consideration of the policies, processes and procedures (controls) within the system used to provide the services. Although the description is generally narrative in nature, there is no prescribed format for the description. In addition, flowcharts, matrices, tables, graphics, context diagrams, or a combination thereof, may be used to supplement the narratives contained within the description.

Additionally, the description can be organized in a variety of different ways. For example, the description may be organized by components of internal control (the control environment, risk assessment process, control activities, monitoring activities and information and communications). Alternatively, it may be organized by components of the system (infrastructure, software, people, data, and processes and procedures) and supplemented by disclosures of the aspects of the internal control components relevant to the identification and assessment of risks that would prevent the service organization from achieving its commitments and system requirements and by disclosures of the design, implementation and operation of controls to address those risks.

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

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

- Describes the system that the service organization has implemented (that is, placed in operation) to provide the services
- Includes information about each description criterion, to the extent it is relevant to the system being described
- Does not inadvertently or intentionally omit or distort information that is likely to be relevant to report users’ decisions
Although the description should include disclosures about each description criterion, such disclosures are not intended to be made at such a detailed level that they might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the service organization’s ability to achieve its service commitments and system requirements. Instead, the disclosures are intended to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks.

A description that (a) states or implies that certain IT components exist when they do not, (b) states or implies that certain processes and controls have been implemented when they are not being performed, or (c) contains statements that cannot be objectively evaluated (for example, advertising puffery) is not presented in accordance with the description criteria. When evaluating whether the description is presented in accordance with the description criteria, service organization management should consider the implementation guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. Because the implementation guidance does not address all possible situations, management should consider the specific facts and circumstances of the service organization when evaluating the description against the description criteria.

Determining whether the description of a service organization’s system is presented in accordance with the description criteria also involves evaluating whether each control stated in the description has been implemented. Controls have been implemented when they have been placed in operation rather than existing only in the description.

Materiality considerations when preparing the description in accordance with the description criteria

As previously discussed, applying the description criteria requires judgment. One of those judgments involves the informational needs of report users.

For most SOC 2® reports, there is a broad range of specified parties. Therefore, the description is intended to meet the common informational needs of the specified parties and does not ordinarily include information about every aspect of the system that may be considered important to each individual report user. However, an understanding of the perspectives and information needs of the broad range of intended SOC 2® report users is necessary to determine whether the description is presented in accordance with the description criteria and is sufficient to meet their needs. As discussed in chapter 1, users of a SOC 2® report are expected to have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide them, among other matters. (See section titled “Intended Users of the SOC 2® Report” in chapter 1 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.)

Because the description presents primarily nonfinancial information, materiality considerations are mainly qualitative in nature and center around whether there are misstatements, or omissions, in the information disclosed that could, individually or in the aggregate, reasonably be expected to influence the decisions of intended users of the SOC 2® report.

Examples of qualitative factors ordinarily considered when determining whether the description is presented in accordance with the description criteria include the following:
• Whether the description of the service organization’s system includes the significant aspects of system processing

• Whether the description is prepared at a level of detail likely to be meaningful to report users

• Whether each of the relevant description criteria in DC section 200 has been addressed without using language that omits or distorts the information

• Whether the characteristics of the presentation are appropriate, given that the description criteria allow for variations in presentation

The following are some examples related to materiality with respect to the description of the service organization’s system.

Example 1 — Example Service Organization uses a subservice organization to perform its back-office functions and elects to use the carve-out method. The description includes information about the nature of the services the subservice organization provides and describes the monitoring and other controls performed at the service organization with respect to the processing performed by the subservice organization. The description includes such information because it is likely to be relevant to report users and, therefore, such information would be considered material to the description of the service organization’s system.

Example 2 — A service auditor is reporting on Example Service Organization’s security controls. The service organization mirrors data to a data center located in another city and creates tapes of the data as a secondary backup. These tapes are stored at a third location. Data written to the backup tapes are encrypted. The service organization has identified the encryption of the tape as a control, but it has not identified physical security controls over the tape storage location as a control because management has concluded that the destruction of both backups simultaneously is remote, and the encryption of the data on the tapes is sufficient. In this example, the omission of controls over physical access is not likely to be material or relevant to report users because controls over the encryption of the tapes prevent unauthorized access to the information and compensate for the omission of controls over physical access to the facility.

Having a reasonable basis for the assertion

Service organization management is responsible for having a reasonable basis for its assertion about the description and the effectiveness of controls stated therein. Furthermore, because management’s assertion generally addresses the suitability of the design of controls and, in a type 2 examination, the operating effectiveness of controls over a period, management’s basis for its assertion covers the same time frame. (The procedures the service auditor performs during a SOC 2® examination are not considered a basis for management’s assertion because the service auditor is not part of the service organization’s internal control.)

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

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

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

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

Service organization management may document the assessment in a variety of ways, including using policy manuals, narratives, flowcharts, decision tables, procedural write-ups or questionnaires. The nature and extent of documentation usually varies, depending on the size and complexity of the service organization and its monitoring activities.

If management does not have 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.

Providing the service auditor with a written assertion

The attestation standards require the service auditor to request a written assertion from the responsible party that addresses all the subject matters in the SOC 2® examination. Specifically, the assertion addresses whether (a) the description presents the system designed and implemented in accordance with the description criteria, (b) the controls were suitably designed to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved, and (c) in a type 2 examination, the controls operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved. Service organization management may use any language in its written assertion if it addresses management’s conclusions about the description, the suitability of controls, and, in a type 2 examination, the operating effectiveness of controls.

Management usually attaches the assertion to the description. Segregating the assertion from the description clarifies that the assertion is not part of the description.

If management refuses to provide the service auditor with a written assertion, the attestation standards require the service auditor to withdraw from the engagement when withdrawal is possible under applicable laws and regulations. If law or regulation does not allow the service auditor to withdraw, the service auditor is required to disclaim an opinion.
Modifying management’s assertion

As previously discussed, management provides the service auditor with a written assertion at the beginning of the SOC 2® examination. However, during the engagement, the service auditor may identify deficiencies or deviations that may cause the service auditor to qualify the opinion. Management’s written 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 after the engagement. (See the section below.)

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 reliably 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.
Endnotes

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 As discussed in paragraph 2.59 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy, controls can only provide reasonable assurance that an organization’s objectives are achieved. In a SOC 2® examination, the service organization designs, implements, and operates controls to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust service criteria.

3 A SOC 2® examination may be performed on any of the trust services categories (security, availability, processing integrity, confidentiality and privacy). Use of the trust services criteria in a SOC 2® examination is discussed beginning in paragraph 1.31 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

4 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.

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 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy discusses these two methods for treating subservice organizations.

6 In the July 2015 version of the SOC 2® guide, these controls were referred to as “controls expected to be implemented at carved-out subservice organizations.”

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

8 If the service organization uses one or more subservice organizations and elects to use the inclusive method for preparing the description, subservice organization management is also a responsible party.

9 This table can also be found in chapter 1 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

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

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

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

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

14 The description criteria presented in DC section 200 (2018 description criteria) have been designed to be used in conjunction with the 2017 trust services criteria set forth in TSP section 100, as discussed in the following footnote. The description criteria included in paragraphs 1.26 and 1.27 of the 2015 AICPA Guide Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (2015 description criteria) are codified as DC section 200A.

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

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

15 The 2017 trust services criteria are codified in TSP section 100. The extant trust services criteria (2016 trust services criteria) are codified in TSP section 100A and will be available through Dec. 15, 2018. Until that date, service auditors may use either the 2016 trust services criteria or the 2017 trust services criteria as the evaluation criteria in a SOC 2® examination. After that date, the 2016 trust services criteria will be considered superseded. During the transition period, management and the service auditor should identify in the SOC 2® report whether the 2017 or 2016 trust services criteria were used.

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

16 This table can also be found in chapter 1 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.
Endnotes (continued)

17 This table can also be found in chapter 1 of AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

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 A85 of AT-C section 205, Examination Engagements, the addition of such information may increase the potential for the report to be misunderstood, which may lead the service auditor to add a restricted-use paragraph to the report; therefore, a SOC 3® report containing such information is unlikely to be appropriate for general use.

20 ICFR stands for internal control over financial reporting.

21 A misstatement is a difference between the measurement or evaluation of the subject matter by the responsible party and the proper measurement or evaluation of the subject matter based on the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions.

22 Controls also may be relevant when they are part of one or more of the other components of a user entity’s internal control over financial reporting. The components of an entity’s internal control over financial reporting are described in detail in the auditing standards with which a service auditor should comply.

23 In the July 2015 version of the SOC 2® guide, those controls were referred to as controls expected to be implemented at carved-out subservice organizations.

24 If the service organization uses a subservice organization and elects the inclusive method, subservice organization management is also a responsible party. Accordingly, subservice organization management also needs to provide written assertions and representations to the service auditor. If subservice organization management refuses to provide a written assertion, service organization management cannot use the inclusive method but may be able to use the carve-out method.