Chapter 1

Introduction and Background

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

Introduction

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

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

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

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

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

- *Enterprise IT outsourcing services*. Managing, operating, and maintaining user entities' IT data centers, infrastructure, and application systems and related functions that support IT activities, such as network, production, security, change management, hardware, and environmental control activities.
- *Managed security*. Managing access to networks and computing systems for user entities (for example, granting access to a system and preventing, or detecting and mitigating, system intrusion).
- *Financial technology (FinTech) services*. Providing financial services companies with IT-based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, crowdfunding, big data analytics, and asset management.

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

1.04 To assess and address the risks associated with a service organization, its services, and the system used to provide the services, user entities and business partners usually need information about the design, operation, and effectiveness of controls[2] within the system. To support their risk assessments, user entities and business partners may request a SOC 2® report from the service organization. A SOC 2® report is the result of an examination of whether (*a*) the description of the service organization's system presents the system that was designed and implemented in accordance with the description criteria, (*b*) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the criteria, if those controls operated effectively, and (*c*) in a type 2 examination, the controls stated in the description operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the criteria relevant to the security, availability, or processing integrity of the service organization's system (security, availability, processing integrity) or based on the criteria relevant to the system's ability to maintain the confidentiality or privacy of the information processed for user entities (confidentiality

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

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

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

a. A type 1 examination is an examination of whether

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

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

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

b. A type 2 examination also addresses the description of the system and the suitability of design of controls, but it also includes an additional subject matter: whether controls operated effectively throughout the period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. A type 2 examination also includes a detailed description of the service auditor's[5] tests of controls and the results of those tests. A report on such an examination is referred to as a *type 2 report*.

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

Intended Users of a SOC 2® Report

1.07 A SOC 2® report, whether a type 1 or a type 2 report, is usually intended to provide report users with information about the service organization's system relevant to security, availability, processing integrity, confidentiality, or privacy to enable such users to assess and address the risks that arise from their relationships with the service organization. For instance, the description of the service organization's system is intended to provide report users with information about the system that may be useful when assessing the risks arising

---

[3] As discussed in paragraph 2.59, controls can only provide reasonable assurance that an organization's objectives are achieved. In a SOC 2® examination, the service organization designs, implements, and operates controls to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria.

[4] A SOC 2® examination may be performed on any of the trust services categories (security, availability, processing integrity, confidentiality, and privacy). Use of the trust services criteria in a SOC 2® examination is discussed beginning in paragraph 1.31.

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

from interactions with the service organization's system, particularly system controls that the service organization has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria. For example, disclosures about the types of services provided, the environment in which the entity operates, and the components of the system used to provide such services allow report users to better understand the context in which the system controls operate.

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

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations[6] and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls[7] and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entities' ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks

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

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

---

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

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

or business partners, who intend to use the information contained in the SOC 2® report as part of their vendor selection process or to comply with regulatory requirements for vendor acceptance, may have gained such knowledge while performing due diligence. (If prospective users lack such knowledge and understanding, management may instead engage a service auditor to provide a SOC 3® report, as discussed in paragraph 1.13.)

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

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

1.13 In some situations, service organization management may wish to distribute a report on the service organization's controls relevant to security, availability, confidentiality, processing integrity, or privacy to users who lack the knowledge and understanding described in paragraph 1.08. In that case, management may engage a service auditor to examine and express an opinion on the effectiveness of controls within a service organization's system in a SOC 3® examination. As discussed beginning at paragraph 1.55, a SOC 3® report is ordinarily appropriate for general users. Chapter 4, "Forming the Opinion and Preparing the Service Auditor's Report," discusses the reporting elements of a SOC 3® report in further detail.

Overview of a SOC 2® Examination

1.14 As previously discussed, a SOC 2® examination is an examination of a service organization's description of its system, the suitability of the design of its controls, and in a type 2 examination, the operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, or privacy. This guide provides performance and reporting guidance for both types of SOC 2® examinations.

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

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

1.16 In a SOC 2® examination, service organization management is the responsible party. However, in certain situations there may be other responsible parties.[9] As the responsible party, service organization management prepares the description of the service organization's system that is included in the SOC 2® report. In addition, the service auditor is required by the attestation standards[10] to request a written assertion from management. Management's written assertion addresses whether (*a*) the description of the service organization's system is presented in accordance with the description criteria, (*b*) the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (*c*) in a type 2 examination, those controls were operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

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

Contents of the SOC 2® Report

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

Table 1-1
Contents of a SOC 2® Report

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

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

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

Contents of a SOC 2® Report—*continued*

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

(continued)

Contents of a SOC 2® Report—*continued*

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

Definition of a System

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

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

- *Infrastructure*. The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services
- *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications
- *People*. The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers)
- *Data*. The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the system

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

Boundaries of the System

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

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

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

Time Frame of Examination

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

Difference Between Privacy and Confidentiality

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

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

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

Criteria for a SOC 2® Examination

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

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

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

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

[13] The description criteria presented in supplement A, "2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report," (2018 description criteria) have been designed to be used in conjunction with the 2017 trust services criteria set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, as discussed in the following footnote. The 2018 description criteria are codified in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the 2015 AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) are

(continued)

Report,[14] which includes the criteria used to prepare and evaluate the description of the service organization's system. The use of these criteria, referred to as the *description criteria,* in a SOC 2® examination is discussed further beginning in paragraph 1.28.

- *Trust services criteria.*[15] Supplement B of this guide presents an excerpt from TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*[16] (the 2017 trust services criteria), which includes the criteria used to evaluate the suitability of the design and, in a type 2 examination, the operating effectiveness of the controls relevant to the trust services category or categories included within the scope of a particular examination. The use of these criteria, referred to as the applicable trust services criteria, in a SOC 2® examination is discussed further beginning in paragraph 1.31.

Description Criteria

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

(footnote continued)

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

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

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

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

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

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

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

1.29 The description criteria in supplement A were promulgated by the Assurance Services Executive Committee (ASEC), which is designated by the Council of the AICPA under the AICPA Code of Professional Conduct to issue measurement criteria. Therefore, such criteria are considered suitable for use in a SOC 2® examination. Because the description criteria are published by the AICPA and made available to the public, they are considered available to report users. Therefore, they meet the definition in paragraph .25*b*ii of AT-C section 105 for criteria that is both suitable and available for use in an attestation engagement.

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

Trust Services Criteria

1.31 The engaging party,[17] typically the responsible party, may choose to engage the service auditor to report on controls related to one or more of the trust services categories (security, availability, processing integrity, confidentiality, and privacy).

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

1.33 Because applying the trust services criteria requires judgment, supplement B also presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control—Integrated Framework*[18] (COSO framework) states that points of focus represent important characteristics of the criteria in that framework. Consistent with the COSO framework, the points of focus in supplement B may assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy. In addition, the points of focus may assist both management and the service auditor when evaluating whether controls stated in the description were suitably designed and operated to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

1.34 As previously discussed, a service organization faces risks that threaten its ability to achieve its service commitments and system requirements. The criterion for determining whether controls are suitably designed is that the controls stated in the description[19] would, if operating as described,

---

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

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

[19] Description criterion DC5 in supplement A indicates that the description of the service organization's system should include the applicable trust services criteria and the related controls designed to meet those criteria.

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

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

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

Categories of Criteria

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

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

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

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

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

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

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

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

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

Common Criteria

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

a. Control environment (CC1 series)

b. Communication and information (CC2 series)

c. Risk assessment (CC3 series)

d. Monitoring activities (CC4 series)

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

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

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

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

Table 1-2
Criteria for Evaluating the Design and Operating Effectiveness of Controls

Trust Services Category	*Common Criteria*	*Additional Category-Specific Criteria*
Security	X	
Availability	X	X
Processing integrity	X	X
Confidentiality	X	X
Privacy	X	X

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

1.43 *Using the Trust Services Criteria to Evaluate Suitability of Design and Operating Effectiveness in a SOC 2® Examination.* As previously discussed, the trust services criteria presented in supplement B are used to evaluate the effectiveness (suitability of design and operating effectiveness) of controls in a

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

The Service Organization's Service Commitments and System Requirements

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

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

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

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

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

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

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

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

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

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

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

Table 1-3

Additional Subject Matter and Additional Criteria

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

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

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

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

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

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

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

SOC 3® Examination

1.55 To market its services to prospective customers of the system, a service organization may want to provide them with a SOC 2® report. However, some of those prospective customers (system users) may not have sufficient knowledge about the system, which might cause them to misunderstand the information in the report. Consequently, distribution of the SOC 2® report for general marketing purposes is likely be inappropriate. In this situation, a SOC 3® report, which is a general use report, may be more appropriate. Because the procedures performed in a SOC 2® examination are substantially the same as those performed in a SOC 3® examination, the service organization may ask the service auditor to issue two reports at the end of the examination: a SOC 2® report to meet the governance needs of its existing customers and a SOC 3® report to meet more general user needs.

1.56 In a SOC 3® examination, service organization management prepares, and includes in the SOC 3® report, a written assertion about whether the controls within the system were effective[20] throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. In connection with the assertion, management also describes (*a*) the boundaries of the system and (*b*) the service organization's principal service commitments and system requirements. Such disclosures, which ordinarily accompany the assertion, enable report users to understand the scope of the SOC 3® examination and how management evaluated the effectiveness of controls. The SOC 3® report also includes the service auditor's opinion on whether management's assertion was fairly stated based on the applicable trust services criteria. As in a SOC 2® examination, a service auditor may be engaged to report on one or more of the five trust services categories included in TSP section 100.

1.57 Unlike a SOC 2® report, a SOC 3® report does not include a description of the system, so the detailed controls within the system are not disclosed. In addition, the SOC 3® report does not include a description of the service auditor's tests of controls and the results thereof.[21] Appendix B, "Comparison of SOC 1®, SOC 2®, and SOC 3® Examinations and Related Reports," compares a SOC 2® and a SOC 3® report.

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

Other Types of SOC Examinations: SOC Suite of Services

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

---

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

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

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

1. SOC 1®—SOC for Service Organizations: ICFR[22]
2. SOC 2®—SOC for Service Organizations: Trust Services Criteria
3. SOC 3®—SOC for Service Organizations: Trust Services Criteria for General Use Report
4. SOC for Cybersecurity

SOC 1®—SOC for Service Organizations: ICFR

1.60 AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, provides performance and reporting requirements for an examination of controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. The controls addressed in AT-C section 320 are those that a service organization implements to prevent, or detect and correct, misstatements[23] in the information it provides to user entities. A service organization's controls are relevant to a user entity's internal control over financial reporting when they are part of the user entity's information and communications component of internal control maintained by the service organization.[24] Such an examination is known as a SOC 1® examination, and the resulting report is known as a SOC 1® report.

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

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

SOC for Cybersecurity

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

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

[23] Paragraph .10 of AT-C section 105, *Concepts Common to All Attestation Engagements*, defines a *misstatement* as a difference between the measurement or evaluation of the subject matter by the responsible party and the proper measurement or evaluation of the subject matter based on the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions. Throughout this guide, the terms *description misstatements*, *deviations*, and *deficiencies* all refer to types of misstatements.

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

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

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

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

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

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

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

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

Professional Standards

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

Attestation Standards

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

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

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

Code of Professional Conduct

1.73 The AICPA Code of Professional Conduct (code) provides guidance and rules that apply to all members in the performance of their professional responsibilities. The code includes the fundamental principles that govern the performance of all professional services performed by CPAs and, among other things, call for CPAs to maintain high ethical standards and to exercise due care in the performance of all services. When providing attestation services, the "Considering or Subsequent Employment or Association With an Attest Client" subtopic (ET sec. 1.279)[25] of the "Independence Rule" (ET sec. 1.200.001) requires CPAs to be independent in both fact and appearance. Independence in a SOC 2® examination is discussed further beginning in paragraph 2.36.

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

Quality in the SOC 2® Examination

1.74 Paragraphs .06–.07 of AT-C section 105 discuss the relationship between the attestation standards and the AICPA quality control standards. Quality control systems, policies, and procedures are the responsibility of a firm when conducting its attestation practice. Under QC section 10, *A Firm's System of Quality Control*,[26] a CPA firm has an obligation to establish and maintain a system of quality control to provide it with reasonable assurance that

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

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

1.75 QC section 10 additionally states that the firm should establish criteria against which all engagements are to be evaluated to determine whether an engagement quality control review should be performed. If the engagement meets the established criteria, the nature, timing, and extent of the engagement quality control review should follow the guidance discussed in that standard and the requirements in paragraph .42 of AT-C section 105.

1.76 Paragraph .33 of AT-C section 105 states that the engagement partner should take responsibility for the overall quality of the attestation engagement, including matters such as client acceptance and continuance, compliance with professional standards, and maintenance of appropriate documentation, among others. As part of those responsibilities, paragraph .32 of AT-C section 105 states that the engagement partner should be satisfied that all members of the engagement team, including external specialists, have the competence and capabilities to perform the engagement in accordance with professional standards. Chapter 2 discusses assessing the competence and capabilities that members of the engagement team need to possess to perform a SOC 2® examination.

Definitions

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

---

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