AICPA®

# Information for Entity Management

# Appendix A

## *Information for Entity Management*

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

The purpose of this document is to assist entity management with understanding its responsibilities in a SOC for Supply Chain examination. It is also intended to provide helpful guidance to entity management when discharging those responsibilities.

## Introduction and Background

Many entities, such as the following, produce, manufacture, or distribute products:

- *Producers.* Producers include entities that extract raw materials through operations that remove metals, minerals, and aggregates from the earth (such as oil and gas extraction, mining, dredging, and quarrying); produce food, feed, fiber and other products by the cultivation of certain plants and the raising of domesticated animals (livestock); and develop software for on-site installation.
- *Manufacturers.* Manufacturers include entities that transform raw materials or components into other components or finished goods for use or sale using labor and machines, tools, chemical and biological processes, fabrication, or formulation. The components or finished goods may be sold to other manufacturers for the production of other products such as aircraft, computers or computer parts, household appliances, furniture, sports equipment or automobiles. In other cases, the finished goods may be sold to wholesalers that, in turn, sell them to retailers that then sell them to end users and consumers. Manufacturers include contract manufacturers that outsource manufacturing for other entities.
- *Commercial software developers.* Commercial software developers are entities that develop and sell commercial software that is offered for sale. Commercial software developers are distinguished from software development service providers that are engaged to create, modify, and implement software to meet a particular entity's needs based on a contract for services. The system that provides software development services is best addressed by a SOC 2® examination.
- *Distribution companies.* Distribution companies include entities that provide or manage all or a significant part of another entity's logistics, including one or a combination of the following: inbound freight, customs, warehousing, inventory management, order fulfillment (including picking and repackaging of items), distribution, or outbound freight. Such companies include third-party logistics (3PL or TPL) companies.

Due to rapid technological advancement, the production, manufacture, or distribution of products often involves a high level of interdependence and connectivity between an entity and (*a*) organizations that supply raw materials or components for the manufacturing process (suppliers)[1] and (*b*) the entity's customers and business partners. These relationships are often considered part of the *supply chain.*

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

- Provide products that meet the principal product performance specifications.
- Meet delivery and quality commitments and requirements.
- Meet production, manufacturing, or distribution commitments and requirements.

For that reason, suppliers, customers, and business partners expect entity management to establish operational and compliance objectives. Such objectives, which are referred to within this guide as *system objectives*, may also change over time because of changing risks and changing laws and regulations.

To identify, assess, and address the risks arising from interactions between the entity and the system it uses to produce, manufacture, or distribute products, suppliers, customers, and business partners usually need information about the design, operation, and effectiveness of controls[2] within the system. To support their risk assessments, they may request an attestation report from the entity. Such a report is the result of an attestation engagement in which a practitioner examines and opines on whether (*a*) the description of the entity's system that produces, manufactures, or distribute products (the *description of the system* or *description*) presents the system that was designed and implemented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria. This examination is referred to as a SOC for Supply Chain examination.

This document is intended to

- assist entity management in preparing its description of the manufacturing, production, or distribution system, which serves as the basis for a SOC for Supply Chain examination.
- familiarize entity management with its responsibilities when it engages a service auditor to perform a SOC for Supply Chain engagement.

[1] As used in this document, a *supplier* is an individual or business (and its employees) that provides products (such as raw materials, components, or other goods) or services to a producer, manufacturer, or distribution company (an entity). A service provider, for example, is a specific type of supplier that provides services to an entity.

[2] In this document, *controls* are policies and procedures that are part of the entity's system of internal control. The objective of an entity's system of internal control is to provide reasonable assurance that system objectives are achieved.

## Intended Users of a SOC for Supply Chain Report

A SOC for Supply Chain report is designed to provide intended users with information about a system that produces, manufactures, or distributes products and the effectiveness of controls within that system (that is, controls related to one or more of the applicable trust services categories of security, availability, processing integrity, confidentiality, or privacy) that are necessary to provide reasonable assurance that the entity's principal system objectives were achieved based on the applicable trust services criteria. The report is designed to provide intended users with information they may use to identify, assess, and manage the risks that arise from their relationships with the entity.

A SOC for Supply Chain report is intended for use by those who have sufficient knowledge and understanding of the entity, the products it produces, manufactures, and distributes, and the system that produces, manufactures, or distributes them. The expected knowledge of intended users ordinarily includes the following:

- The nature of the goods produced, manufactured, or distributed by the entity
- Internal control and its limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the entity's principal system objectives and how controls address those risks

Without such knowledge, users are likely to misunderstand the content of the report, the assertions made by entity management, and the practitioner's opinion, all of which are included in the SOC for Supply Chain report. For that reason, the practitioner's report is required to be restricted to intended users who possess that knowledge. In addition, entity management and the practitioner ordinarily would agree on the intended users of the report.

The following intended users are presumed to have the requisite knowledge:

*a.* Business customers, including immediate customers or similar business entities further down the supply chain that do the following:

   i. Use the system's products as components of their production and manufacturing systems (for example, production machinery)

   ii. Use the system's products as inputs to their products (for example, computers used in automobiles)

   iii. Use the system's products as a part of their service delivery (for example, IV bags used by a hospital)

   iv. Resell the products

   v. Rely on a physical distribution system for products used as inputs to other products

   Business customers need information about the entity's system, including the nature and effectiveness of controls within that system, to understand the entity's controls and to determine whether those controls, in addition to their own controls, are sufficient to mitigate their business risks.

*b.* Business partners that

i. are dependent on the entity for sales of the business partners' goods or

ii. license the use of the business partner's intellectual property to the entity.

Business partners may include affiliated organizations that are customers or suppliers of the entity. Business partners need information about the entity's system and the controls within that system to manage and assess the risks associated with doing business with the entity.

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

Parties other than those identified in this document may also have the requisite knowledge and understanding. For example, prospective customers and business partners may have gained such knowledge while performing their supplier selection processes or while assessing a supplier's compliance with regulatory requirements. In addition, nonregulatory, standard-setting bodies consisting of business customers or business partners that represent their membership (for example, industry consortiums) may also have the requisite knowledge. If they have the requisite knowledge, prospective customers and business partners and nonregulatory standard-setting bodies may be intended users of the report.

As previously discussed, the SOC for Supply Chain report has been designed to meet the common information needs of intended users described in this section. However, nothing precludes the practitioner from restricting the use of the practitioner's report to a smaller subset of intended users.

## Overview of a SOC for Supply Chain Examination

The practitioner performs a SOC for Supply Chain examination in accordance with the AICPA's attestation standards. Those standards establish performance and reporting requirements for the 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.

Entity management is usually the responsible party. However, in certain situations, there may be other responsible parties. As the responsible party, entity management prepares the description of the entity's system that is included in the SOC for Supply Chain report. In addition, the practitioner should request from the responsible party a written assertion about the measurement or evaluation of the subject matter against the criteria. Management's written assertion, which is included in the SOC for Supply Chain report, addresses whether (*a*) the description of the entity's system is presented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective throughout the period based on the applicable trust services criteria.

The practitioner designs and performs procedures to obtain sufficient appropriate evidence to support an opinion about whether (*a*) the description presents the system that was designed and implemented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective during the period based on the applicable trust services criteria, in all material respects. As discussed in the subsequent section, the practitioner also presents, in a separate section of the report, a description of the practitioner's tests of controls and the results thereof.

## Contents of the SOC for Supply Chain Report

A SOC for Supply Chain examination results in the issuance of a SOC for Supply Chain report. The SOC for Supply Chain report includes four key components:

1. Entity management's description of the system the entity uses to produce, manufacture, or distribute products in accordance with the description criteria
2. Entity management's assertion about whether, in all material respects,
    a. the description of the entity's system is presented in accordance with the description criteria and
    b. the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective throughout the period, based on the applicable trust services criteria
3. The practitioner's opinion about whether, in all material respects,
    a. the description of the entity's system is presented in accordance with the description criteria and
    b. the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective throughout the period, based on the applicable trust services criteria
4. The practitioner's description of the procedures performed and the results thereof

## Description Criteria for Preparation of the Description of an Entity's System

DC section 300, *2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report,*[3] includes the description criteria to be used by entity management to prepare and evaluate the description of the entity's system. Supplement A presents an excerpt from that document.

Applying the description criteria in actual situations requires judgment. Therefore, implementation guidance is included 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, management

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

needs to consider the facts and circumstances of the entity and its environment when applying the description criteria.

## The Trust Services Criteria for Evaluation of Control Effectiveness

TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* (the 2017 trust services criteria)[4] includes the control criteria used to evaluate the effectiveness of controls relevant to the trust services category or categories included within the scope of a specific examination. Supplement B presents an excerpt from that document.

Because applying the trust services criteria requires judgment, that document also includes 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.[5] Consistent with the COSO framework, the points of focus 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 entity management when evaluating whether controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria. The trust services criteria are discussed in more detail later in this appendix.

## The Entity's System Objectives and Principal System Objectives

An entity adopts a mission and vision, sets strategies, and establishes objectives to help it meet its mission and vision based on its strategies. Management designs and implements individual production, manufacturing, or distribution systems to achieve certain specific objectives (referred to as *system objectives*) and controls within the system to mitigate the risks that would prevent the entity from achieving those objectives.

A SOC for Supply Chain examination addresses the system objectives that could reasonably be expected to influence the relevant decisions of the intended users. These system objectives, referred to as *principal system objectives*, typically address the category or categories addressed by the examination and relate to achieving commitments, specifications, or requirements. Management discloses its principal system objectives in the system description. When evaluating the effectiveness of controls, management makes that evaluation in light of what the system controls were designed to achieve: the principal system objectives.

As discussed earlier, an entity's principal system objectives are those that could reasonably be expected to influence relevant decisions made by intended users.

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

[5] ©2020 Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved.

Typically, an entity's principal system objectives relate to achieving commitments, specifications, or requirements. An entity's commitments often relate to meeting the product's specifications and meeting other production, manufacturing, and distribution specifications. Commitments may also relate to other matters (for example, conforming with a variety of other standards and criteria such as the risk entity management framework issued by the National Institute of Standards and Technology [NIST], the cybersecurity standards issued by the International Organization on Standardization [ISO], or the Food and Drug Administration regulations in Code of Federal Regulations (CFR), *Electronic Records; Electronic Signatures*, Title 21, Part 11). An entity may also make commitments about different aspects of the product or its distribution, including commitments related to a product's performance specifications and availability.

Table 1 illustrates the types of matters that are likely to be addressed by principal system objectives established by entity management, depending on the trust services category or categories addressed by the examination.

## Table 1

**Types of Matters Addressed by Principal System Objectives by Trust Services Category**

| ***Trust Services Category*** | ***Matters That Might Be Addressed by the Entity's Principal System Objectives*** |
|---|---|
| **Security** | Commitments regarding the protection of the system from physical and logical (including cybersecurity) risks |
| **Availability** | The product's availability in the quantities and at the times agreed on with customers |
| | The achievement of delivery commitments made to customers, including the timing of delivery, storage and transportation commitments, and the system requirements necessary to achieve those commitments (for example, commitments made to a pharmaceutical company related to the maintenance of products at specific temperatures during the distribution process) |
| | Distribution of the product in accordance with applicable laws and regulations regarding timing, storage, and transportation |
| **Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)** | The system's ability to produce products that achieve product performance specifications (the physical characteristics or functionality of a product) |

*(continued)*

**Types of Matters Addressed by Principal System Objectives by Trust Services Category — *continued***

| *Trust Services Category* | *Matters That Might Be Addressed by the Entity's Principal System Objectives* |
|---|---|
| | The system's ability to achieve other commitments made to customers |
| | The system's conformity with production requirements established by the entity to meet or comply with laws or regulations, industry standards, or customers' requirements (for example, a manufacturer may be contractually required to perform certain industry-standard quality control testing during the production process) |
| **Confidentiality** | The achievement of specific commitments made to customers or business partners (for example, commitments made to a business partner regarding the entity's use of the business partner's intellectual property during the production process) |
| **Privacy** | The achievement of commitments and system requirements identified in the entity's privacy notice or privacy policy |

Entity management is responsible for designing, implementing, and operating a system and related controls that are necessary to obtain reasonable assurance of achieving its principal system objectives based on the applicable trust services criteria. It is also responsible for disclosing, in the description, the entity's principal system objectives with sufficient clarity to enable intended users to understand how the system operates and how entity management and the practitioner evaluated the effectiveness of controls.

## Matters Not Addressed by a SOC for Supply Chain Examination

As discussed in the prior section, the examination may address one or more of the trust services categories. When the examination addresses processing integrity, the practitioner's opinion addresses, among other things, whether system controls were effective to provide reasonable assurance that goods produced or manufactured meet their product performance specifications.

However, the practitioner's opinion does not address whether the goods produced by the system are free from defect or whether they will function as designed. In other words, the practitioner's opinion is not a *warranty* or *guarantee* that the goods produced will meet product performance specifications or other commitments made to customers. Therefore, the practitioner's opinion does not address whether the products are fit for purpose or merchantable.

## Entity Management Responsibilities Prior to Engaging the Practitioner

Entity management is responsible for having a reasonable basis for asserting that the system and related controls provide reasonable assurance that the system objectives it has established are achieved. The basis for management's belief is based, in part, on management having:

*a.* identified the principal system objectives.

*b.* identified and analyzed the risks that threaten the achievement of those principal system objectives.

*c.* designed, implemented, and operated controls that are necessary to provide reasonable assurance that the principal system objectives were achieved based on the applicable trust services criteria.

Prior to engaging a practitioner to perform the examination, entity management is responsible for making a variety of decisions that affect the scope of the examination, including the following:

*a.* Identifying the goods produced, manufactured, or distributed by the entity to which the examination relates

*b.* Identifying the components of the system to be examined

*c.* Identifying the boundaries of that system

*d.* If the examination is intended to meet the needs of business partners as well as those of customers, identifying the risks arising from the entity's responsibilities to business partners providing intellectual property or components used by the production or manufacturing system, if any

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

*f.* Determining the period of time to be addressed by the examination

Before entity management can fulfill those responsibilities, entity management may need clarification of certain matters from the practitioner. For example, entity management may have questions about whether certain processes or components are considered part of the system to be examined or about the effect of a supplier's controls on the entity's ability to achieve its principal system objectives.

## Defining the System to Be Examined

The subject matter of the SOC for Supply Chain engagement revolves around the system and related controls that the entity has designed, implemented, and operated to manufacture, produce, or distribute goods. The examination is flexible in terms of addressing any of the following:

- A system and controls that an entity uses to produce, manufacture, or distribute a physical (for example, an airplane engine) or intangible product (for example, a commercial off-the-shelf application)
- All systems and controls that an entity uses to operate a production line

- All systems and controls that an entity uses to produce, manufacture, or distribute goods produced or manufactured within a specific facility or physical plant

There may be circumstances in which entity management may not be prepared to make an assertion about whether the controls within the entity's system were effective to achieve the entity's principal system objectives. In such circumstances, rather than making an assertion about whether controls were effective to achieve the entity's principal system objectives, entity management makes an assertion only about the suitability of the design of implemented controls. An examination on such an assertion is referred to as a design-only examination and includes consideration of the following: (1) whether the description of the entity's system was presented in accordance with the description criteria and (2) whether implemented controls stated in the description were suitably designed to achieve the entity's principal system objectives, if the controls operated effectively. A design-only examination may be useful to intended users who want to obtain an understanding of the entity's system and the controls the entity has implemented to achieve its principal system objectives. However, it would not provide intended users with sufficient information to assess the effectiveness of controls within the entity's system.

Entity management is responsible for identifying the specific subject matter to be examined, which includes identifying the components of the system and the boundaries of the system to be examined. Management is also responsible for establishing its principal system objectives and selecting the trust services category or categories to be addressed by the examination, as well as selecting the period of time to be addressed. The following paragraphs provide a brief overview of each of these factors and how they might affect the subject matter of the engagement.

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 objectives (for example, objectives that address the production or delivery of goods) in accordance with management-specified requirements. System components can be classified into the following five categories: (1) infrastructure, (2) software, (3) people, (4) data, and (5) procedures. For a manufacturing or production system, for instance, infrastructure would include the components of the manufacturing system and the processes by which they operate. Although inputs, such as raw materials, are not a component of the system, they are often necessary for a product to be produced or manufactured. For that reason, raw materials and other inputs (for example, purchased components) are often important in the production or manufacturing process and, therefore, are disclosed in the description in addition to the components of the system.

Determining the functions or processes that are outside the boundaries of the system being examined, and describing them in the description, is often necessary to prevent intended users from misunderstanding the description of the system and the practitioner's opinion. Therefore, if there is a risk that users might be confused about whether a specific function or process is part of the system being examined, the description needs to clarify which processes or functions are within the scope of the examination and which are not.

For example, the following functions or processes at the entity may be outside the boundaries of the system being examined because they are unlikely to be relevant to the achievement of the principal system objectives related to security, availability, processing integrity, confidentiality and privacy:

- The process used to invoice customers for the products manufactured by the entity
- The processes used to collect and report on sustainability matters that do not directly affect the finished product

In an examination that addresses security and availability, for example, the system boundaries ordinarily would cover, at a minimum, all the system components as they relate to the production or manufacturing process, beginning with the receipt of the raw materials or components, throughout the production of the goods, to the transfer of finished goods to a third-party logistics company for distribution to customers or to the customers themselves. The system boundaries would ordinarily not address ancillary functions, such as the combination of production information with other information for secondary purposes internal to the entity (for example, customer metrics tracking and financial reporting systems).

When the examination addresses processing integrity, and the practitioner believes that the product itself may not meet its product performance specifications, the practitioner may need to consider the suitability of the design of the system. In that situation, the system being examined may need to include controls over system design as they relate to the system's ability to produce a product that meets its product performance specifications. If the system was designed during a period prior to the start of the examination period, the practitioner may consider whether controls that operated in the examination period, such as controls over customer complaints and other controls used to monitor products for design flaws, are effective to adequately identify flaws in the suitability of the system's design.

If embedded logic is a part of the product (for example, microcode in a CPU chip), that logic is provided by a carved-out supplier, and the description does not contain a clear indication that production of the embedded logic is the responsibility of the carved-out supplier and, thus, outside the boundaries of the system, the practitioner may conclude that the absence of such information is a misstatement. In such instances, the practitioner evaluates whether the misstatement is material to the decisions of report users and would result in the description being misleading.

In an examination that addresses confidentiality or privacy, 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 confidential or personal information by well-defined processes and informal ad hoc procedures.

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

In addition to identifying the components of the system, it is also necessary to consider which trust services category or categories are to be addressed by the examination. As previously discussed, the trust services criteria are used to measure the effectiveness of controls in a SOC for Supply Chain examination, and the examination can address any or all of the trust services categories of security, availability, processing integrity, confidentiality, or privacy.

In most cases, the examination would address the category or categories that would best meet the information needs of intended users. Often, which categories those are is determined by considering the commitments the entity makes to its customers and business partners.

Because of the increased dependence on technology and concerns about cybersecurity risks, security is likely to be addressed in most examinations performed using the trust services criteria. Often, customers and business partners of an entity are also interested in the effectiveness of controls over availability because such controls may be integral to meeting their commitments. For instance, a customer that relies on airbags manufactured by the entity is likely to want information about the processes and controls the entity has designed and implemented and operates to achieve the availability commitments it makes to its customers. For those reasons, a SOC for Supply Chain examination that addresses both security and availability is likely to meet the information needs of intended users as a group.

In some cases, intended users may also be interested in the processing integrity of the system the entity uses to produce, manufacture, or distribute goods, including the processing integrity of the components of that system (for example, hardware, tooling, software, and information). Processing integrity addresses system controls that mitigate the risk that the entity's system objectives will not be achieved because of failures in the production process. Assume that a product contains embedded logic (for example, firmware of an embedded computer) necessary to achieve one or more of the entity's principal system objectives, and the embedded logic is the subject of ongoing service commitments the entity makes to its customers and business partners. In that case, intended users may be interested in the process and controls the entity has designed and implemented and operates to achieve the processing integrity of the system, which includes the parts of the production system that are part of the products themselves (for example, microcode in a CPU chip). Thus, an examination that addresses processing integrity, in addition to security and availability, may best meet the needs of those intended users.

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

## Categories of Trust Services Criteria

The trust services criteria relate to 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 achieve its objectives.

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

*c*. *Processing integrity (over the provision of services or the production, manufacturing, or distribution of goods)*. System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives. (In a SOC for Supply Chain examination, the term *processing integrity* relates to production processing. In other words, production processing is complete, valid, accurate, timely, and authorized to produce, manufacture, or distribute goods that meet the entity's specifications.)

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

*e.* *Privacy*. Personal information is collected, used, retained, disclosed, and disposed of to achieve 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

*a.* criteria common to all five trust services categories (common criteria) and

*b.* additional specific control activity criteria relevant to the categories of availability, processing integrity, confidentiality, or privacy.

For example, if an examination addresses only availability, the controls tested would be those that address all the common criteria and the criteria for availability.

The common criteria provide specific criteria for addressing the control environment (CC1 series), communication and information (CC2 series), risk assessment (CC3 series), monitoring of controls (CC4 series), and control activities related to the design and implementation of controls (CC5 series). These criteria are the principles of internal control set forth in the COSO framework. In addition to the COSO principles, the common criteria are supplemented with specific criteria for control activities addressing general IT controls over logical and physical access (CC6 series), system operations (CC7 series), change management (CC8 series), and risk mitigation (CC9 series).

The AICPA's Assurance Services Executive Committee has determined that the common criteria are suitable for evaluating the effectiveness of controls necessary to provide reasonable assurance that an entity achieves its principal system objectives related to security; no additional control activity criteria are needed. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria and (*b*) the control activity criteria applicable to the specific category. Table 2 identifies the trust services criteria to be addressed when evaluating the effectiveness of controls for each of the trust services categories.

## Table 2

**Criteria for Evaluating the Design and Operating Effectiveness of Controls**

| ***Trust Services Category*** | ***Common Criteria*** | ***Additional Category-Specific Criteria*** |
|---|---|---|
| Security | X | |
| Availability | X | X (A series) |
| Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods) | X | X (PI series) |
| Confidentiality | X | X (C series) |
| Privacy | X | X (P series) |

Entity management needs to identify the specific risks that threaten the achievement of the principal system objectives and the controls necessary to provide reasonable assurance that those objectives are achieved based on the category or categories to be addressed by the examination.

Entity management is responsible for evaluating whether controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective throughout the period based on the trust services criteria relevant to the trust services categories addressed by the examination. Such criteria are referred to throughout this document as the *applicable trust services criteria*. For example, in an examination that addresses security, the trust services criteria relevant to security, which are the common criteria (CC1.1–CC9.2) are the applicable trust services criteria.

### Determining the Time Frame for the Examination

The subject matter of an attestation examination may be "as of a point in time" or "for a period of time." Entity management is responsible for determining the time frame to be addressed by the examination. Generally, a SOC for Supply Chain examination addresses the effectiveness of controls over a specified period of time. In addition, the guidance in this document is based on the assumption that the period of time over which the effectiveness of controls will be evaluated is the same period of time addressed by the description of the entity's system.

## Identifying Customer Responsibilities and Complementary Customer Controls

Customers often have a role in a production, manufacturing, or distribution process. Fulfilling those responsibilities is necessary for the customer to meet its goals in using an entity as a supplier or distributer. For example, the customer of a logistics company that provides fulfillment services is responsible for providing complete and accurate recipient information and for communicating the items to be packaged and delivered. Such responsibilities are referred to in this document as *customer responsibilities*.

In most cases, the successful performance of these customer responsibilities is not necessary for the entity to achieve its principal system objectives. In certain circumstances, however, a customer must have controls in place to provide reasonable assurance that certain of these customer responsibilities are performed in a defined manner for the entity to achieve its principal system objectives. Such controls are referred to as *complementary customer controls* (CCCs). CCCs are usually presented in tabular format toward the end of the description, along with the trust services criteria to which each CCC relates.

In some situations, it may appear that a customer responsibility is a CCC; however, a thorough analysis of the facts may not support that conclusion. This might be true even in circumstances in which customers have some ability to control portions of the process. For example, a manufacturer may permit a customer's employees to access its information systems and alter its production schedules. If a customer access administrator is responsible for issuing employee credentials, and all actions performed by customer employees are the responsibility of the customer, the achievement of the entity's principal system objectives will not depend on the authorized and appropriate use of the customer employee credentials based on trust services criterion CC6.2, which states, "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."

If a customer responsibility is not a CCC, it usually would not be disclosed in the description; rather, it would usually be communicated through product documentation or user manuals. However, entity management would ordinarily identify in the description the types of communications it makes to external parties.

When entity management communicates customer responsibilities only to certain intended users (for example, in contracts with customers), entity management considers whether other potential users are likely to misunderstand the report. In such situations, it may be necessary to restrict the use of the report to specified users. If entity management does not want to limit the use of the report to a subset of intended users, entity management would identify the significant customer responsibilities in the description to enable intended users to understand the subject matter and the related practitioner's opinion. In that case, the report would be appropriate for intended users.

## Identifying Suppliers and Complementary Supplier Controls

### Suppliers Whose Controls Are Necessary for the Entity to Achieve Its Principal System Objectives

An entity that produces, manufactures, or distributes products obtains raw materials, components, or other goods (for example production equipment) from suppliers. It may also outsource various processing functions (such as the provision of IT networks) to service providers. In this appendix, the term *supplier* is used to refer to suppliers, vendors, and service providers (and their employees) that provide products (such as raw materials, components, or other goods) or services to the entity. A supplier may be a separate entity that is external to the entity or may be a related entity, for example, a subsidiary of the same company that owns the entity.

In most cases, an entity is likely to have effective controls over the quality of products and services provided by critical suppliers to provide reasonable assurance of achieving its principal system objectives. If that is the case, it may not be necessary for the intended users to understand the supplier's controls because those controls are not necessary for the entity to achieve its principal system objectives. Examples of situations in which an entity may have effective controls over a supplier's goods or services to achieve its principal system objectives include the following:

- An entity has a robust quality-inspection process for all inputs to the system, which is executed upon receipt of goods from the supplier. The process includes inspection of shipping containers and boxes for physical damage, statistical selection of sample inputs for measurement against input specifications and requirements, and visual inspection of inputs by production personnel. In this case, the entity's controls are sufficient to reduce the risk that inputs do not comply with specifications.

- An entity has robust controls, including change management controls, over a system that a supplier uses to produce new software, which the entity then uses in its production process. In that case, the entity's third-party risk and control assessment activities are sufficient for the entity to achieve its principal system objectives.
- A supplier is responsible for performing quarterly maintenance on an entity's backup power system in an examination that addresses availability. If the entity implements its own third-party risk and control assessment activities over the supplier's controls, then the supplier's controls would not be necessary for the entity to achieve its principal system objectives.
- An entity outsources its application development testing to a supplier and stipulates in its supplier contract that the supplier is responsible for performing certain controls the entity believes are necessary to address the risks related to doing business with the supplier. The entity designates an entity employee to oversee the outsourced services, and that employee compares the supplier's test plans, test scripts, and test data to the entity's application change requests and detailed design documents. The designated entity employee also reviews the results of testing performed by the supplier before changes to the application are approved by the supplier and submitted to the entity for user acceptance testing. The supplier's controls may not be necessary for the entity to assert that its controls provide reasonable assurance that the entity's principal availability commitments were achieved based on the applicable trust services criteria.

## Complementary Supplier Controls

In other situations, however, the entity may delegate certain responsibilities to the supplier and expect the supplier to perform specific controls over the processes that produce or deliver goods and services received. As a result, effective supplier controls may be necessary for the entity to achieve its principal system objectives. For example, an entity may be unable to monitor controls at an infrastructure-as-a-service provider designed to maintain the confidentiality of a business partner's proprietary information. In another example, an original equipment manufacturer customer may specify that the entity needs to obtain a specific component from a specific customer-approved manufacturer and that the entity should accept the component "as is."

When the controls performed by the supplier are necessary, in combination with the entity's controls, to achieve the entity's principal system objectives, such controls are referred to as complementary supplier controls (CSCs). Because of the importance of CSCs to report users, they are disclosed in the description. The most common method for presenting CSCs is to define the system by including only those processes and controls whose performance is the responsibility of the entity and to identify in the description the CSCs that the entity expects suppliers to implement. This is known as the *carve-out method*.

When using the carve-out method, the description identifies the types of CSCs that the supplier is assumed to have implemented and the trust services criteria affected by them. CSCs are usually presented in tabular format toward the end of the description, along with the trust services criteria to which each CSC relates. Entity management may request the practitioner's assistance when determining how to present the CSCs in the description. The practitioner can provide examples of CSC disclosures made by other entities and can make recommendations to improve the presentation of the CSCs in the description.

## Using the Inclusive Method

In some situations, because of the significance of a supplier's role in the production, manufacturing, or distribution process, entity management may elect to present the relevant processes and controls of the supplier in its description. This method of presentation is known as the *inclusive method*. Under the inclusive method, the description of the entity's system includes certain disclosures related to the nature of the products or services obtained from the supplier and the components of the supplier's system, including the related controls. When using the inclusive method, the supplier's system components and controls are subject to the practitioner's examination procedures.

When the inclusive method is used, supplier management is also a responsible party in the examination and has to fulfill many of the same requirements as entity management, including providing the practitioner with a written assertion and representation letter at the end of the examination. Therefore, use of the inclusive method involves extensive planning and communication among the practitioner, entity management, and the supplier.

The use of the inclusive method becomes more complex when the entity uses multiple suppliers whose controls are necessary, in combination with the entity's controls, for the entity to provide reasonable assurance that its principal system objectives are achieved. When the controls of more than one supplier are likely to be relevant to report users, entity management may elect to use the inclusive method for one or more suppliers and the carve-out method for others. In these instances, the description needs to clearly state which suppliers and related functions and processes are included within the scope of the examination and which are carved out.

Because of the additional complexities involved with the use of the inclusive method, both entity and supplier management may agree on the use of the inclusive approach during engagement acceptance. In addition, to facilitate the process, entity management generally coordinates the use of the inclusive method with supplier management. If the inclusive method is used, matters to be agreed on or coordinated include the following:

*a.* The scope of the examination and the period to be covered by the practitioner's report

*b.* Acknowledgment from supplier management that it will provide the practitioner with a written assertion and representation letter

*c.* The planned content and format of the inclusive description

*d.* The representatives of the supplier and the entity and who will be responsible for

   i. providing each entity's description and

   ii. integrating the descriptions

*e.* The timing of the tests of controls

During planning, the practitioner may discuss such matters with entity management. At that time, the practitioner may also discuss whether he or she believes it will be possible to obtain evidence that supports the portion of the opinion that relates to the supplier's controls.

The practitioner determines whether supplier management will provide a written assertion and representation letter. In addition, the practitioner determines whether it will be possible to obtain evidence that supports the portion of the opinion that addresses the supplier. If entity management wishes to use the inclusive method, but supplier management refuses to provide a written assertion, the entity will not be able to use the inclusive method.

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

As a responsible party, supplier management is also responsible for the following:

*a.* Designing, documenting, implementing, and operating controls that are suitably designed and operating effectively

*b.* Having a reasonable basis for its assertion

*c.* Providing the practitioner with written representations at the end of the engagement

*d.* If the practitioner plans to use internal auditors to provide direct assistance, providing the practitioner with written acknowledgment that internal auditors providing direct assistance to the practitioner will be allowed to follow the practitioner's instructions and that the supplier will not intervene in the work the internal auditors perform for the practitioner

*e.* Providing the practitioner with the following:

  i. Access to all information, such as records, documentation, service level agreements, and internal audit or other reports, that supplier management is aware of and that is relevant to the description of the supplier's system and assertion

  ii. Access to additional information that the practitioner may request from supplier management for the examination

  iii. Unrestricted access to supplier personnel from whom the practitioner determines it is necessary to obtain evidence relevant to the examination

*f.* Disclosing to the practitioner the following:

  i. Incidents (that are clearly not trivial) on the part of the supplier or its employees of noncompliance with laws and regulations, fraud, or uncorrected misstatements related to the system or goods produced, manufactured, or distributed, and whether such incidents have been communicated appropriately to affected parties

  ii. Incidents (that are clearly not trivial) at its suppliers or business partners of noncompliance with laws and regulations, fraud, or uncorrected misstatements related to the system or goods produced, manufactured, or distributed of which supplier management is aware

iii. Knowledge of any actual, suspected, or alleged intentional acts that could adversely affect the description of the supplier's system or the effectiveness of controls

iv. Any deficiencies in the design of controls of which supplier management is aware

v. All instances in which controls have not operated as described

vi. All identified system incidents that resulted in a significant impairment of the supplier's commitments to the entity and its customers during the period of time covered by the description

vii. Any events subsequent to the period covered by the description of the system, up to the date of the practitioner's report, that could have a significant effect on the description, the design or operation of the controls, or management's assertion

Supplier management's assertion ordinarily would be expected to address the same matters addressed by entity management in its assertion, including the effectiveness of controls and whether the description presents the system the supplier uses to produce, manufacture, or distribute products to the entity and its customers in accordance with the description criteria. However, in some cases, entity management might design the controls for the supplier. When entity management designs the controls for the supplier, entity management takes responsibility for the suitability of the design of its own controls and the supplier 's controls; therefore, the supplier's assertion may be limited to whether the description presents the system that it uses to produce, manufacture, or distribute products to the entity and its customers in accordance with the description criteria and whether the controls at the supplier operated as described.

## Agreeing on the Terms of the Engagement

The attestation standards require the practitioner to agree on and document the terms of the engagement with the engaging party. A written agreement, such as an engagement letter, reduces the risk that either the practitioner or entity management may misinterpret the needs or expectations of the other party. For example, it reduces the risk that entity management may rely on the practitioner to protect the entity against certain risks or to perform certain management functions.

The agreed-upon terms of the engagement should include the following:

*a.* The objective and scope of the engagement

*b.* The responsibilities of the practitioner

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

*d.* The responsibilities of the responsible party and the 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 practitioner with a representation letter at the conclusion of the engagement

If the practitioner plans to use internal auditors to provide direct assistance, prior to doing so, the practitioner may also obtain written acknowledgment from the responsible party (usually entity management) that internal auditors providing direct assistance to the practitioner will be allowed to follow the practitioner's instructions and that the responsible party will not intervene in the work the internal auditors perform for the practitioner. If the engaging party is the responsible party, the practitioner may wish to include this matter in the engagement letter. In addition to the matters discussed in the previous two paragraphs, the practitioner may also want to reach an understanding with entity management about other matters, such as a draft of principal system objectives identified by entity management.

Although not required by the attestation standards, the practitioner would ordinarily request a signed engagement letter from the engaging party. The engaging party's refusal to provide the practitioner with an engagement letter may cause the practitioner to question whether a mutual understanding regarding the terms of the engagement has been reached and, in turn, may affect the practitioner's decision about whether to accept or continue the engagement.

## Entity Management Responsibilities During the Examination

In a SOC for Supply Chain engagement, entity management is responsible for the following:

*a.* Preparing a description of the entity's system in accordance with the description criteria

*b.* Providing a written assertion that accompanies the description of the entity's system, both of which will be provided to report users

*c.* Having a reasonable basis for its assertion

*d.* If the practitioner plans to use internal auditors to provide direct assistance, providing the practitioner with written acknowledgment that internal auditors providing direct assistance to the practitioner will be allowed to follow the practitioner's instructions and that the entity will not intervene in the work the internal auditors perform for the practitioner

*e.* Providing the practitioner with the following:

   i. Access to all information, such as records, documentation, service level agreements, and internal audit or other reports, that management is aware of and that are relevant to the description of the entity's system and assertion

   ii. Access to additional information that the practitioner may request from management

iii. Unrestricted access to personnel within the entity from whom the practitioner determines it is necessary to obtain evidence relevant to the SOC for Supply Chain examination

*f.* Disclosing to the practitioner the following:

i. Incidents (that are clearly not trivial) on the part of the entity or its employees of noncompliance with laws and regulations, fraud, or uncorrected misstatements related to the system or goods produced, manufactured, or distributed and whether such incidents have been communicated appropriately to affected parties

ii. Incidents (that are clearly not trivial) at suppliers or business partners of noncompliance with laws and regulations, fraud, or uncorrected misstatements related to goods produced, manufactured, or distributed or to the system of which it is aware

iii. Knowledge of any actual, suspected, or alleged intentional acts that could adversely affect the presentation of the description of the entity's system or the effectiveness of controls

iv. Any deficiencies in the design of controls of which it is aware

v. All instances in which controls have not operated as described

vi. All identified system incidents that resulted in a significant impairment of the entity's achievement of its principal system objectives during the period of time covered by the description

Entity management may, at the practitioner's request, acknowledge these responsibilities in an engagement letter or other suitable form of written communication.

## Preparing the Description of the Service Organization's System

As previously discussed, the description of the entity's system presented in accordance with the description criteria is designed to enable customers, business partners, and others to better understand the entity's system. Among other things, the description provides information about the risks that threaten the achievement of the entity's principal system objectives and the procedures and controls the entity has implemented to manage those risks. For example, disclosures about the types of products produced, manufactured, or distributed by an entity; the characteristics of the production, manufacturing, or distribution processes; the technical environment in which the entity operates; and the components of the system that produces, manufactures, or distributes the entity's products allow users to better understand the context in which the system controls operate.

Entity management is responsible for preparing the description of the system that was designed and implemented in accordance with the description criteria presented in supplement A, "2020 Description Criteria for a Description of an

Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report." The practitioner is responsible for determining whether the description is prepared in accordance with the description criteria.

Generally, entity management prepares the description from documentation supporting the system and system operations and from consideration of the policies, processes, and procedures (controls) within the system. There is no prescribed format for the description. Entity management may organize the description in a variety of ways, provided that disclosures called for by the description criteria are included. Flowcharts, matrixes, tables, graphics, context diagrams, or a combination thereof may be used to supplement the narratives contained within the description.

The extent of disclosures included in the description may vary depending on the size and complexity of the entity and its activities. In addition, the description need not address every aspect of the entity's system for producing, manufacturing, or distributing goods, particularly if certain aspects of the system are not relevant to intended users or are beyond the scope of the SOC for Supply Chain examination. For example, disclosures about an entity's processes related to billing customers for the manufactured products are unlikely to be relevant to report users. Similarly, although the description may address procedures within both manual and automated systems by which products are produced, manufactured, or distributed, it need not necessarily disclose every step in those processes.

Nevertheless, the disclosures are expected to be made at a level of detail that could reasonably be expected to meet the common information needs of intended users. As an example, assume an entity uses a supplier to provide its computer processing infrastructure and includes the following disclosure in the description:

> The Entity outsources aspects of its computer processing to Computer Outsourcing Associates.

In this situation, entity management may consider whether more extensive disclosures, such as the following, might be more useful:

> The Entity hosts its ERP System at Computer Outsourcing Associates. The Entity maintains responsibility for application changes and user access, and Computer Outsourcing Associates provides the computer processing infrastructure and changes thereto.

Although the description is expected to include relevant disclosures addressing 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 entity's ability to achieve its principal system objectives. Instead, the disclosures are intended to enable intended users to understand the nature of the risks faced by the entity and the potential impact of the realization of those risks.

When evaluating whether the description is presented in accordance with the description criteria, entity management and the practitioner may consider the following:

## Table 3

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

| *Characteristics That May Indicate the Description Is Presented in Accordance With the Description Criteria* | *Characteristics That May Indicate the Description Is Not Presented in Accordance With the Description Criteria* |
|---|---|
| The description describes the significant aspects of the system the entity has designed and implemented (placed into operation) to produce, manufacture, or distribute the products. | The description states or implies that certain IT components exist when they do not. |
| The description does not inadvertently or intentionally omit or distort information that is likely to be relevant to intended users' decisions. | The description states or implies that certain processes and controls were implemented when they were not being performed. |
| The description includes information about each description criterion, to the extent it is relevant to the system being described, without using language that omits or distorts the information. | The description contains statements that cannot be objectively evaluated (for example, advertising puffery). |
| The description is prepared at a level of detail likely to be meaningful to intended users as a group. | The description is prepared at such a high level that it omits significant amounts of information relevant for decision-making by intended users. |
| The characteristics of the presentation, such as the format, are appropriate, given that the description criteria allow for variations in presentation. | Certain characteristics of the presentation of the description are confusing and obscure critical information about the system. |

When evaluating whether the description is presented in accordance with the description criteria, entity management may also 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. The implementation guidance does not address all possible situations; therefore, entity management needs to consider the facts and circumstances of the entity and its environment when applying the description criteria.

In certain circumstances, additional disclosures may be necessary to supplement the description. Entity management's decisions about whether such additional disclosures are necessary, and the practitioner's evaluation of entity management's decisions, involve consideration of whether the disclosures may affect information that is likely to be relevant to the decisions of intended users. Examples of additional disclosures that may be necessary include the following:

*a.* Significant interpretations made in applying the description criteria in the specific circumstances of the examination (for example, what constitutes a security event or incident)

*b.* Subsequent events, depending on their nature and significance

If the practitioner identifies description misstatements (including omissions) in the description that the practitioner believes may be material, the practitioner usually asks entity management to revise the description. In most situations, entity management makes the appropriate modifications to align the assertion to the opinion. If, however, entity management does not appropriately modify the description to address the practitioner's concerns, the practitioner would evaluate whether the misstatement is material and determine the effect of the misstatement on his or her opinion on the description.

## Disclosures Required by Description Criteria

### *DC1: Disclosures Related to the Types of Goods Produced, Manufactured, or Distributed*

Description criterion DC1 requires entity management to include in the description certain disclosures about the types of goods produced, manufactured, or distributed by the entity and, if relevant, the characteristics of the production, manufacturing, or distribution processes. Description criterion DC1 contains implementation guidance that is intended to assist practitioners when evaluating the nature and extent of disclosures about the types of goods produced, manufactured, or distributed.

### *DC2: Disclosures About the Entity's Principal System Objectives*

As previously discussed, management is responsible for designing, implementing, and operating a system and related controls that are necessary to obtain reasonable assurance of achieving the principal system objectives it has identified based on the applicable trust services criteria. Identifying the principal system objectives is part of the entity's risk assessment process and is necessary for an effective system of internal control.

Intended users need to understand the relationship between the principal system objectives identified by management and the trust services criteria to understand how the effectiveness of controls was evaluated; therefore, description criterion DC2 requires entity management to disclose the principal system objectives in the description. An entity's principal system objectives generally address the system's ability to meet product performance specifications, commitments, and requirements, and production, manufacturing, or distribution commitments and requirements. The principal system objectives are those that are relevant to the trust services category or categories addressed by the description and likely to affect relevant decisions of intended users of the report.

### *DC3: Disclosures About System Incidents*

Description criterion DC3 requires entity management to include in the description certain information related to system incidents that were the result of controls that were not effective or otherwise resulted in a significant failure in the achievement of one or more principal system objectives. Specifically, the description is expected to include the following information about each incident:

*a.* Nature of each incident

*b.* Timing surrounding the incident

*c.* Extent (or effect) of the incident and its disposition

Description criterion DC3 contains implementation guidance that is intended to assist practitioners when evaluating the nature and extent of disclosures about system incidents. The following is an example of disclosures about an identified system incident:

> During the period under assessment, the Company experienced an incident in which an online intruder gained access to the server used to store and configure the embedded software used in its widgets. Through a previously unknown operating system vulnerability in the server used to update the supplier's software, the intruder made unauthorized changes to the software and configuration parameters to be loaded in the widgets. The attack was detected approximately 66 hours after the unauthorized access was obtained and was remediated within 5 days of detection. The Company ceased the manufacturing of widgets during the 5-day period and recalled all widgets that were loaded with the software from the time of initial unauthorized access through the remediation of the incident. The Company reconciled serial numbers of all recalled and unshipped widgets to manufacturing records without exception. Based on this reconciliation, management believes that all widgets with the unauthorized software have been accounted for. All of these widgets were subsequently destroyed under controlled conditions.
>
> As part of the remediation, the Company reinstalled the operating system and applications from a backup made prior to the incident and applied the software patch provided by the operating system supplier.

### *DC4: Disclosures About Significant Risks That Affect the Entity's Production, Manufacturing, or Distribution*

Description criterion DC4 requires entity management to include in the description certain information related to significant risks that affect the entity's production, manufacturing, or distribution. Description criterion DC4 contains implementation guidance that is intended to assist practitioners when evaluating the nature and extent of disclosures about significant risks.

### *DC5: Disclosures About Inputs to and Components of the System*

Description criterion DC5 requires entity management to include in the description certain information related to inputs to the system (raw materials and other inputs) and the components of the system that produces, manufactures, or distributes the product. Description criterion DC5 also contains implementation guidance that is intended to assist practitioners when evaluating the nature and extent of disclosures about inputs to and components of the system.

### *DC6: Disclosures About Individual Controls and the Applicable Trust Services Criteria*

Description criterion DC6 requires disclosure of the applicable trust services criteria (that is, those that relate to the categories addressed by the description) and the related controls that are necessary to provide reasonable assurance that the entity's principal system objectives were achieved. For example, if the description addresses availability, entity management would provide information about the controls it has implemented to address the common criteria in the trust services criteria and the additional trust services criteria for availability.

The description is expected to disclose only implemented controls. For those implemented controls, the description provides sufficient details about those controls to enable intended users, particularly customers and business partners, to understand how such controls may affect their interactions with the entity. Table 4 presents information about each control that generally would be included in the description. Boldface italics in the right-hand column of the table indicate text that specifically answers the questions posed in the left-hand column.

## Table 4

**Disclosures About Controls to Be Included in the Description**

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

**Disclosures About Controls to Be Included in the Description — *continued***

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

*(continued)*

**Disclosures About Controls to Be Included in the Description — *continued***

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

Although entity management may describe the controls in the description, it also might refer to a table of controls (such as the preceding table) and present it in a separate section of the report. If the description refers to a table of controls, the table is considered part of the description; therefore, it is also addressed by the practitioner's examination. Often, the practitioner describes the tests of controls performed and the results thereof in the same table.

An entity may have controls it considers to be outside the boundaries of the system addressed by the description, such as controls related to the conversion of new customers to the entity's systems. To avoid misunderstanding by report users, the description is expected to clearly delineate the boundaries of the system included within the scope of the examination.

### *DC7: Disclosures About Complementary Customer Controls and Customer Responsibilities*

When CCCs are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved, description criterion DC7 requires certain disclosures about the CCCs to be included in the description. Description criterion DC7 also contains implementation guidance that is intended to assist practitioners when evaluating the nature and extent of disclosures about significant risks.

CCCs are typically identified by management when it assesses the risks that threaten the achievement of its principal system objectives and determines that the mitigation of those risks depends on controls to be performed by customers. Entity management will usually provide the practitioner with its risk assessment, which identifies such CCCs. If entity management's process is informal, the practitioner may need to perform additional procedures, such as an independent assessment of risk that includes the CCCs.

## DC8: Disclosures Related to Suppliers

When controls performed by the supplier are necessary, in combination with the entity's controls, to achieve the principal system objectives, description criterion DC8 requires certain disclosures about the supplier; the nature of such disclosures varies depending on the method selected by management for making those disclosures.

### Disclosures When Using the Carve-Out Method

When controls performed by the supplier are necessary, in combination with the entity's controls, to achieve the principal system objectives, such controls are referred to as complementary supplier controls (CSCs). The most common method for presenting CSCs in the description is to include only those processes and controls whose performance is the responsibility of the entity and to identify the CSCs that the entity expects suppliers to implement. This method is known as the carve-out method.

When the carve-out method is used, DC8 requires disclosure of the following information:

*a.* The nature of the raw materials or components produced, manufactured, or distributed, or the services provided by, the supplier

*b.* Each of the applicable trust services criteria intended to be met by the supplier's controls

*c.* The types of CSCs that entity management assumed, in the design of the entity's system, would be implemented by the supplier and that are necessary, in combination with controls at the entity, to provide reasonable assurance that the entity's principal system objectives are achieved

DC8 also contains implementation guidance that is intended to assist practitioners when evaluating the nature and extent of disclosures about suppliers when the carve-out method is used.

To be meaningful to report users, CSCs described in the description are expected to include those that are specific to the raw materials or components produced, manufactured, or distributed, or the services provided by, the supplier. Typically, entity management presents the CSCs as broad categories of controls or types of controls that the supplier is expected to have in place. For example, the entity might identify the following CSC to address trust services criterion CC6.1, *The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives*:

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

Because CSCs are necessary, in combination with the entity's controls, to provide reasonable assurance that certain principal system objectives are achieved, it is important that the description also include the supplier's responsibilities for implementing them and indicate that the entity can only achieve the related principal system objectives if suitably designed CSCs are effective throughout the period. CSCs are also considered when evaluating the suitability of design of controls.

### *Disclosures When Using the Inclusive Method*

In some situations, entity management may wish to present the relevant processes and controls of the supplier in its description to meet the common information needs of users or because of the significance of the supplier's role in the entity's production, manufacturing, or distribution process. This method of presentation is known as the inclusive method. Under the inclusive method, the relevant aspects of the supplier's infrastructure, software, people, procedures, and data are considered part of the entity's system; therefore, they are disclosed in the description and are subject to the practitioner's examination procedures. The description separately identifies controls at the entity and controls at the supplier. However, there is no prescribed format for differentiating between the two.

When the inclusive method is used, supplier management is also a responsible party in the examination. Because of the additional complexities involved with the use of the inclusive method, entity and supplier management usually agree on the use of the inclusive approach during engagement acceptance.

When the inclusive method is used to present the services provided by a supplier, DC8 requires disclosure of the following information:

*a.* The nature of the raw materials or components produced, manufactured, or distributed, or the services provided by, the supplier

*b.* The portions of the system that are attributable to the supplier

*c.* Relevant aspects of the supplier's infrastructure, software, people, procedures, and data

*d.* The controls at the supplier that are necessary, in combination with the entity's controls, to provide reasonable assurance that the entity's principal system objectives were achieved based on the applicable trust services criteria

The description of the supplier controls may also include aspects of the supplier's control environment, risk assessment process, information and communications, and monitoring activities to the extent that they are relevant to the entity's controls. The description is expected to differentiate between entity controls and supplier controls; however, there is no prescribed format for doing so.

DC8 also contains implementation guidance that is intended to assist practitioners when evaluating the nature and extent of disclosures about suppliers when the inclusive method is used.

### *Considerations Applicable to Both Methods*

Regardless of the method selected by management, the description of the entity's system and the scope of the practitioner's examination would include a description of the controls designed, implemented, and operated at the entity to monitor the effectiveness of the supplier's controls. That is because monitoring controls over suppliers are usually a necessary part of a system of internal control to provide reasonable assurance that the entity's principal system objectives were achieved. These types of controls are evaluated based on trust services criterion CC9.2, *The entity assesses and manages risks associated with vendors and business partners*.

### DC9: Disclosures About Nonrelevant Criteria

Description criterion DC9 requires the description to disclose any specific applicable trust services criterion that is not relevant to the system being described and the reasons it is not relevant. For example, an applicable trust services criterion may not be relevant if it does not apply to the production, manufacturing, or distribution system being examined.

### DC10: Disclosures About Significant Changes to the System During the Period

Description criterion DC10 requires disclosure of significant changes to the entity's system during the period addressed by the description that are relevant to the achievement of the entity's principal system objectives. Significant changes to be disclosed consist of those that are likely to be relevant to intended users.

## Materiality Considerations When Preparing the Description in Accordance With the Description Criteria

As discussed previously, management makes an assertion about whether the description presents the system that has been designed and implemented in accordance with the description criteria. A misstatement in the description, however, may be caused by any of the following:

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

Because the description of the system is a narrative presentation, considering materiality involves some unique judgments. Therefore, when making decisions about the nature and extent of disclosures to include in the description, entity management needs to consider the needs of intended users of the report.

Entity management may also consider certain qualitative factors when evaluating whether the disclosures included in the description are in accordance with the description criteria. Examples of such factors may include the following:

- The characteristics of the presentation, such as format, adopted for the description because the description criteria allow for variations in presentation
- Whether the wording chosen with respect to disclosures required by the description criteria omits or distorts the information
- Whether a misstatement is the result of an intentional act or is unintentional (for example, if the practitioner believes entity

management omitted certain disclosures to portray the system in a better light)

- Considering whether information about certain aspects of the subject matter addressed in the description is likely to be more important to intended users. Examples include the following:
  - Recent national media coverage about the scarcity of replacement airbags may cause the practitioner to consider criteria-required disclosures related to a supplier's controls around the availability of its products likely to be more significant to intended users of a report of a car manufacturer whose airbags for a specific line of vehicles have recently been recalled than criteria-required disclosures related to the supplier's controls around confidentiality.
  - Because personal health information (PHI) is frequently targeted by hackers, the practitioner may consider disclosures required by the description criteria related to security included in a report on the entity's security, availability, and confidentiality controls likely to be more significant to intended users of the report when the report is for a manufacturer of medical devices that uses PHI than when the report is for a wholesaler of surgical garments.

The following examples illustrate materiality considerations of entity management when deciding what to disclose in the description of the entity's system:

> *Example 1.* Example Entity uses a service provider to perform its back-office functions and elects to use the carve-out method. The description includes information about the nature of the services provided by the service provider and describes the monitoring and other controls performed at the entity with respect to the processing performed by the service provider. The description includes such information because it is likely to be relevant to intended users and, therefore, such information would be considered material to the description of the entity 's system.
>
> *Example 2.* Example Entity manufactures running shoes at three different facilities within the United States: Coos Bay, Oregon; Naperville, Illinois; and Iowa City, Iowa. The Oregon and Naperville facilities use the same manufacturing control system, 1Run. The Iowa facility uses a separate control system, Hawkeyes, that is segmented from the 1Run system. In total, 80% of Example Entity's shoes are manufactured in Oregon and 18% are manufactured in Illinois. The Iowa location manufactures less than 5% per year, and for the last three years has been averaging just 2% of shoe production. Thus, Example Entity has identified the Oregon and Illinois facilities as being within the scope of the report and has concluded that the Iowa facility is not material to the overall manufacturing of running shoes and will not be included in the report scope. The entity disclosed these details within the report and indicated that the Hawkeyes manufacturing system is not included within the boundaries of the system being examined.

## Providing a Written Assertion

The attestation standards require the practitioner to request a written assertion from the responsible party that addresses the subject matter of the engagement. In the examination discussed in this guide, the responsible party's assertion addresses whether (*a*) the description presents the system designed and implemented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria.

Entity management's assertion is included in the SOC for Supply Chain report along with the description and the practitioner's opinion. Because management's assertion plays an important role in the engagement, entity management may request that the practitioner provide an example of a written assertion prior to engagement acceptance. However, entity management is responsible for drafting its written assertion and may word the assertion in accordance with its practices, as long as the assertion addresses management's conclusions about the matters discussed in (*a*) and (*b*) of the previous paragraph.

### Having a Reasonable Basis for the Evaluation of Control Effectiveness

Along with its assertion about whether the description presents the system designed and implemented in accordance with the description criteria, entity management also has to provide an assertion about whether the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria (control effectiveness).

To make an assertion about control effectiveness, entity management has to have a reasonable basis for its assertion. Because of the relationship between (*a*) the effectiveness of controls and (*b*) monitoring controls, the practitioner ordinarily discusses with entity management the basis for its assertion prior to engagement acceptance. This assists in determining whether the basis appears reasonable for the size and complexity of the entity and whether the practitioner expects to be able to obtain sufficient appropriate evidence to arrive at an opinion, which is also a precondition of the examination.

Entity management's basis for its assertion usually relies heavily on the entity's monitoring activities. Such monitoring activities typically include ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are ordinarily built into the entity's normal recurring activities. Monitoring activities are particularly important because the entity frequently interacts with customers, business partners, suppliers, and others who have access to the entity's system or otherwise transmit information on behalf of the entity or back and forth between themselves and the entity.

If controls at third parties are necessary, in combination with the entity's controls, to provide reasonable assurance that the entity's principal system objectives are achieved, entity management identifies and assesses the risks of doing business with those third parties. If those risks represent a significant threat to the achievement of the entity's principal system objectives (for example, because of the nature of those parties' access to the system, the provision of critical raw materials or components, or the controls they operate on behalf of the entity), third-party risk and control assessment activities addressing the third parties' activities are necessary to enable entity management to determine whether the processes and controls performed by those third parties effectively mitigate the identified risks. For example, third-party risk and control assessment activities for a supplier may include a combination of the following:

- *a.* Quality control testing of raw materials, components, or other inputs received
- *b.* Testing of controls at the supplier by entity personnel or third parties
- *c.* Holding periodic discussions with supplier personnel and evaluating supplier performance against established service level objectives and agreements
- *d.* Making site visits to the supplier to evaluate its processes
- *e.* Inspecting attestation reports (such as type 2 SOC 2® reports) on the supplier's system
- *f.* Monitoring external communications, such as complaints from customers, entity communications about system events, communications from regulators, and regulatory activities that relate to the products or services provided by the supplier

When such third-party risk and control assessment activities do not exist or they appear inadequate, it may be difficult for entity management to conclude that it has a reasonable basis for its assertion.

If the practitioner believes that entity management does not have a reasonable basis for its assertion, or that sufficient appropriate evidence to support the basis is unlikely to be available, the practitioner ordinarily would not accept the examination.

## Entity Management's Responsibilities During Engagement Completion

Toward the end of the engagement, entity management also has the following responsibilities:

- *a.* Modifying the description, if necessary
- *b.* Considering whether to modify the written assertion
- *c.* Providing the practitioner with written representations
- *d.* Disclosing to the practitioner any events subsequent to the period covered by the description of the system, up to the date of the practitioner's report, that could have a significant effect on the description, the design or operation of the controls, or management's assertion

### Considering Whether Entity Management Should Modify Its Assertion

As previously discussed, entity management provides the practitioner with a written assertion about whether the description presents the system that was designed and implemented in accordance with the description criteria and whether the controls stated in the description were effective. Entity management's written assertion is generally expected to align with the practitioner's opinion by reflecting the same modifications.

## Providing Written Representations

During the examination, entity management makes many oral and written representations to the practitioner in response to specific inquiries or through the presentation of the description and entity management's assertion. Such representations from entity management are part of the evidence the practitioner obtains. However, they cannot replace other evidence the practitioner 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 practitioner has received reliable written representations does not affect the nature or extent of other evidence that the practitioner obtains.

It is up to the practitioner to determine the appropriate person or persons within the entity's management or governance structure with whom to interact, taking into consideration which person or persons have the appropriate responsibilities for and knowledge of the matters concerned. In certain circumstances, the practitioner may obtain written representations from parties in addition to entity management, such as those charged with governance.

In some cases, the party making the assertion may be indirectly responsible for and knowledgeable about specified matters covered in the representations. For example, an entity's chief information officer may be knowledgeable about certain matters through personal experience and about other matters through employees who report to her. The practitioner may request that individuals who are directly or indirectly responsible for and knowledgeable about matters covered in the written representations provide their own representations.

Written representations ordinarily confirm representations explicitly or implicitly given to the practitioner, 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. The written representations, which are usually in the form of a letter from the responsible party, should do the following:

*a.* Include entity management's assertion about each of the subject matters[6] based on the relevant criteria.

*b.* State that

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

   ii. all known matters contradicting the subject matters or assertion and any communication from regulatory agencies or others affecting the subject matters or assertion have been disclosed to the practitioner, including communications received between the end of the period addressed in the written assertion and the date of the practitioner's report.

*c.* Acknowledge responsibility for

[6] Within this section of the document, the term *subject matters* refers to the subject matters in the SOC for Supply Chain examination: (1) the description and (2) the effectiveness of controls.

   i. the subject matters and the assertion,
   ii. selecting the criteria, and
   iii. determining that such criteria are appropriate for entity management's purposes.

*d.* State that entity management has provided the practitioner with all relevant information and access.

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

*f.* State that entity management has disclosed to the practitioner the following, when appropriate:

   i. Incidents (that are clearly not trivial) on the part of the entity or its employees of noncompliance with laws and regulations, fraud, or uncorrected misstatements related to the system or goods produced, manufactured, or distributed and whether such incidents have been communicated appropriately to affected parties
   ii. Incidents (that are clearly not trivial) at suppliers or business partners of noncompliance with laws and regulations, fraud, or uncorrected misstatements related to goods produced, manufactured, or distributed or to the system, of which it is aware
   iii. Knowledge of any actual, suspected, or alleged intentional acts that could adversely affect the subject matters
   iv. Any deficiencies in the design of controls of which it is aware
   v. All instances in which controls have not operated as described
   vi. All identified system incidents that resulted in a significant impairment of the entity's achievement of its principal system objectives during the period of time covered by the examination
   vii. Any events subsequent to the period covered by the description of the system, up to the date of the practitioner's report, that could have a significant effect on the description, the effectiveness of controls, or management's assertion

Other matters about which the practitioner may request representations generally depend on the facts and circumstances of the engagement. For instance, if the entity detected a significant production quality matter prior to distributing the goods, the practitioner may decide to request a representation regarding this and other similar matters.

The written representations required are separate from, and in addition to, entity management's written assertions. The representations are also dated as of the date of the practitioner's report and address the subject matters and periods referred to in the practitioner's opinion.

If an entity uses a supplier, and entity management has elected to use the inclusive method to describe the raw materials, components, or services received from the supplier, the practitioner would also request many of the same representations listed in the previous paragraphs from management of the supplier.

### Requested Written Representations Not Provided or Not Reliable

The attestation standards provide guidance to the practitioner when

*a.* entity management has not provided one or more of the requested representations;

*b.* the practitioner concludes that there is sufficient doubt about the competence, integrity, ethical values, or diligence of those providing the written representations; or

*c.* the practitioner concludes that the written representations are otherwise not reliable.

In such circumstances, the guidance states that the practitioner should

*a.* discuss the matter with the appropriate party or parties,

*b.* reevaluate the integrity of those from whom the representations were requested or received and evaluate the effect that this may have on the reliability of representations and evidence in general, and

*c.* if any of the matters are not resolved to the practitioner's satisfaction, take appropriate action.

### Representations From the Engaging Party When Not the Responsible Party

When the engaging party is not the responsible party, the attestation standards require the practitioner to request written representations from the engaging party, in addition to those requested from the responsible party, in the form of a letter addressed to the practitioner. Those representations should do the following:

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

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

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

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

*e.* State that the engaging party has disclosed to the practitioner all known events subsequent to the period (or point in time) of the subject matter being reported on that would have a material effect on the subject matter or assertion.

*f.* Address other matters as the practitioner deems appropriate.

## Modifying the Assertion

As previously discussed, entity management provides the practitioner with a written assertion about whether the description presents the system that was designed and implemented in accordance with the description criteria and whether the controls stated in the description were effective. Entity management's written assertion is generally expected to align with the practitioner's opinion by reflecting the same modifications.

If the practitioner identifies a misstatement in the description or a deficiency in controls that is determined to be material to the description or to the conclusion on control effectiveness, entity management would consider modifying the assertion to align with the practitioners' opinion. If entity management is unwilling to modify its assertion to align with the practitioner's opinion, the practitioner is required to consider the implications for the practitioner's opinion. For example, the practitioner would consider whether intended users are likely to misunderstand a SOC for Supply Chain report that includes entity management's assertion and the practitioner's opinion when entity management and the practitioner have reached and expressed in the same document different conclusions with respect to the description or the effectiveness of controls. If the practitioner believes it is likely that such a report will be misunderstood by report users, the practitioner may decide to withdraw from the engagement.

## 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 a service organization's, 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[7]
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

Each of those engagements is discussed in the following paragraphs. In addition, appendix B provides a comparison of a SOC for Supply Chain examination and related report with a SOC 2® examination and a SOC for Cybersecurity examination and related reports.

### 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*,[8] 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

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

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

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 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. 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 2® — SOC for Service Organizations: Trust Services Criteria

An entity's management is responsible for assessing and addressing risks faced by the entity related to reporting, compliance with laws and regulations, and the efficiency and effectiveness of its operations. When an entity engages a service provider (referred to as a *service organization* in this context) to perform certain processes or functions, the entity (referred to as a *user entity*) exposes itself to additional risks related to the service organization's system. Although management of a user entity can delegate tasks or functions to a service organization, the ownership and responsibility for the product or service provided to customers of the user entity cannot be delegated. Management of the user entity is held responsible by those charged with governance (for example, board members), customers, shareholders, regulators, and other affected parties for establishing effective internal control over outsourced functions.

To assess and address the risks associated with an outsourced service, management of the user entity needs information about the service organization's controls over the system through which the services are provided. When assessing controls at a service organization that may be relevant to and affect the services provided to user entities, management of a user entity may ask the service organization for a service auditor's report on a description of the service organization's system and the design and operating effectiveness of controls over the service organization's system that may be relevant to the security, availability, or processing integrity of the system or the system's ability to maintain the confidentiality or privacy of the information processed for user entities. Obtaining a service auditor's report from a service organization provides management of the user entity with information that may be useful in assessing risk but does not relieve the user entity of its responsibilities with regard to an effective system of internal control.

In a SOC 2® engagement, the service auditor examines and reports on management's description of a service organization's system and the suitability of the design and operating effectiveness of the controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy against the trust services criteria in TSP section 100. 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 to service auditors engaged to perform a SOC 2® engagement.

## SOC 3® — SOC for Service Organizations: Trust Services Criteria for General Use Report

Similar to a SOC 2® engagement, in a SOC 3® examination the practitioner reports on whether controls within the system, which are necessary to provide reasonable assurance that the service organization achieved its service commitments and system requirements, were effective based on the applicable trust services criteria. Although the requirements and guidance for performing a SOC 3® examination are similar to a SOC 2® examination, the reporting requirements are different. Because of the different reporting requirements, a SOC 2® report is appropriate only for specified parties with sufficient knowledge and understanding of the service organization and the system, whereas a SOC 3® report is ordinarily appropriate for general use.

## SOC for Cybersecurity

Cybersecurity has become a top concern for boards of directors and senior executives of many entities, regardless of their size or the industry in which they operate. 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 SOC for Cybersecurity 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, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*. 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: (1) the description of the entity's cybersecurity risk management program, (2) 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 (3) 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). 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.

AICPA®