Chapter 1

Introduction and Background

This chapter explains the relationship between an *entity*[1] that produces, manufactures, or distributes *products* and its *suppliers*, customers, and *business partners*; provides examples of such entities and the products they produce, manufacture, or distribute; explains the relationship between the products and the *system* that produces, manufactures, or distributes them; describes the components of the system and its boundaries; identifies the *criteria* used to evaluate a description of an entity's system (description criteria); and identifies the criteria (*applicable trust services criteria*) used to evaluate whether *controls* stated in the description, which are necessary to provide reasonable assurance that an entity achieved its *principal system objectives*, were effective. This chapter also provides an overview of a *SOC for Supply Chain examination* and the standards under which the examination is performed. In addition, it provides an overview of other SOC services.

Introduction

1.01 Manufacturing is the production of goods or products[2] for use or sale using labor and machines, tools, chemical and biological processing, or formulation. The term *manufacturing* is most commonly applied to industrial production, in which inputs such as raw materials and components are transformed into finished goods on a large scale. Finished goods may be sold directly to (*a*) end users (for example, medical devices sold to health systems); (*b*) other manufacturers who produce other, more complex products (for example, aircraft, household appliances, furniture, sports equipment, or automobiles); or (*c*) wholesalers, who in turn sell the goods to retailers, who then sell them to end users and consumers.

1.02 A manufacturing (or production) process refers to the steps through which inputs are transformed into a finished good. The manufacturing process begins with the product design and materials specification from which the product is made. The raw materials (including components) are then modified through manufacturing processes to become the finished good.

1.03 Once the goods are manufactured or produced, entities may use systems to distribute the products to customers (for example, an entity[3] that distributes feature films or game DVDs). In contrast, entities may contract with a third-party logistics company to manage the distribution of their products (for example, an air bag manufacturer that contracts with a company to manage its inventory shipment of replacement airbag components to auto repair shops).[4]

[1] Terms defined in appendix F, "Definitions," are italicized on first mention within the text of this guide.

[2] Throughout this guide, the terms *goods* and *products* are used interchangeably.

[3] As used in this guide, an *entity* produces or manufactures goods or provides distribution services for goods.

[4] Paragraph 1.35 provides considerations to help a practitioner determine whether to use the guidance in this guide or that in AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* when engaged to examine and opine on a system and controls of a distributor.

1.04 Distribution companies are entities that use systems to distribute goods produced or manufactured by others. In some cases, they may repackage goods produced or manufactured by others before transporting them to the final customers. In other cases, they may only provide transportation services for products manufactured or produced by others (for example, an express shipping company).

1.05 Examples of entities that may produce, manufacture, or distribute products include the following:

- *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. 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.

1.06 Due to rapid technological advancement, the production, manufacturing, or distribution of products often involves a high level of interdependence and connectivity between the entity and (*a*) organizations that supply raw materials or components for the manufacturing process (suppliers)[5] and (*b*) its customers and business partners. These relationships are often considered part of the *supply chain*. A supply chain is a system of organizations, people, activities, information, and resources involved in moving a product from supplier

[5] In this guide, 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 distributor (an entity). A service provider, for example, is a specific type of supplier that provides services to an entity.

to customer. Supply chain activities involve the transformation of natural resources, raw materials, and components into finished goods. In sophisticated supply chain systems, used products may reenter the supply chain at any point where residual value is recyclable.

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

1.08 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.

1.09 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*[6,7] within the system. To support their risk assessments, suppliers, customers, or business partners may request an attestation report from the entity. Such a report is the result of an attestation engagement in which a *practitioner* examines and opines on (*a*) whether the description of the entity's system that produces, manufactures, or distributes products (the *description of the system* or *description*) presents the system that was designed and implemented in accordance with the description criteria[8] and (*b*) whether the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives,[9] were effective throughout the period, based on the applicable trust services criteria.[10] This examination, referred to as a SOC for Supply Chain examination, or the examination, is the subject of this guide.

[6] In this guide, *controls* are policies and procedures that are part of the entity's system. The objective of an entity's system is to provide reasonable assurance that system objectives are achieved. System objectives are discussed further beginning at paragraph 1.59.

[7] Throughout this guide, the term *effectiveness* (as it relates to controls) encompasses both the suitability of design and the operating effectiveness of controls to provide reasonable assurance that system objectives are achieved.

[8] The *description criteria* are discussed further beginning at paragraph 1.44.

[9] The objective of an entity's system is to provide reasonable assurance that the entity's system objectives are achieved. System objectives are discussed further beginning at paragraph 1.59.

[10] Supplement B of this guide presents an excerpt from TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (the 2017 trust services criteria), which includes the criteria used to evaluate the effectiveness of controls relevant to the trust services category or categories included within the scope of a specific examination. The use of these criteria, referred to as the *applicable trust services criteria*, is discussed further beginning in paragraph 1.44.

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

Intended Users of a SOC for Supply Chain Report

1.10 A *SOC for Supply Chain report* is designed to provide intended users with information about a system an entity uses to produce, manufacture, or distribute products and the effectiveness of controls within that system (that is, controls related to one or more of the applicable trust services categories — security, availability, processing integrity, confidentiality, or privacy) to provide reasonable assurance that the entity's principal system objectives are achieved based on the applicable trust services criteria. The report is also 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.

1.11 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, or distributes; and the system that produces, manufactures, or distributes them. The expected knowledge of intended users ordinarily includes the following:

a. The nature of the goods produced, manufactured, or distributed by the entity

b. *Internal control* and its limitations

c. The applicable trust services criteria

d. The risks that may threaten the achievement of the entity's principal system objectives and how controls address those risks

1.12 Without such knowledge, intended 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. Restricting the use of a practitioner's report in a SOC for Supply Chain examination is discussed beginning in paragraph 4.30. In addition, entity management and the practitioner ordinarily would agree on the intended users of the report.

1.13 In a SOC for Supply Chain report, the following intended users are presumed to have the knowledge identified in paragraph 1.11:

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 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 partners' 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.

1.14 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 as discussed in paragraph 1.11.

1.15 Parties other than those identified in paragraphs 1.13–.14 may also have the requisite knowledge and understanding identified in paragraph 1.11. 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.

1.16 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

1.17 The practitioner performs a SOC for Supply Chain examination in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*.[11] 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.

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

1.18 In a SOC for Supply Chain examination, entity management is usually the responsible party. However, in certain situations, there may be other responsible parties.[12] 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 entity management a written assertion about the measurement or evaluation of the subject matter against the criteria.[13] 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.

1.19 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 throughout the period based on the applicable trust services criteria. As discussed beginning in paragraph 1.20, 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

1.20 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

[12] If the entity uses a supplier and elects to use the inclusive method for preparing the description, supplier management is also a responsible party. Entity management's and the practitioner's responsibilities when the entity uses one or more suppliers and elects to use the inclusive method are discussed further in chapter 2, "Accepting and Planning a SOC for Supply Chain Examination."

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

4. The practitioner's description of the procedures performed and the results thereof[14,15]

1.21 The practitioner's opinion is discussed beginning in paragraph 1.63, and the criteria used in the examination are discussed beginning in paragraph 1.44.

Defining the System to Be Examined

1.22 The subject matter of the examination discussed in this guide 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 [COTS] application)
- Systems and controls that an entity uses to operate a production line
- Systems and controls that an entity uses to produce, manufacture, or distribute goods produced or manufactured within a specific facility or physical plant

1.23 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. Entity 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.

1.24 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) that are important in the production or manufacturing process are often disclosed in the description in addition to the components of the system.

[14] According to paragraph .A85 of AT-C section 205, the addition of procedures performed and the results thereof in a separate section of an examination report may increase the potential for the report to be misunderstood when taken out of the context of the knowledge of the requesting parties. For that reason, a practitioner's report that contains a description of procedures and results is usually restricted to intended users who are likely to understand it.

[15] A description of procedures performed and results thereof would not be included in a design-only examination. A design-only examination is discussed beginning at paragraph 1.41.

1.25 Determining the functions or processes that are outside the boundaries of the system being examined, and describing them in the description, is also necessary to prevent intended users from misunderstanding the description of the system and the practitioner's opinion. Therefore, if there is a risk that intended 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.

1.26 Understanding the components of the system to be examined and the boundaries thereof is also important to the practitioner because it affects how the subject matter will be evaluated against the criteria, the nature of the practitioner's examination procedures, and other matters. Describing the system to be examined is discussed in further detail beginning at paragraph 2.28; discussing the boundaries of the system is addressed beginning at paragraph 2.31. The following paragraphs provide guidance on other matters that might affect the subject matter of a specific engagement.

The Entity's System Objectives and Principal System Objectives

1.27 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 designs and implements controls within the system to mitigate the risks that would prevent the entity from achieving those objectives.

1.28 A SOC for Supply Chain examination addresses the system objectives that could reasonably be expected to influence the relevant decisions of intended users. These system objectives, referred to as *principal system objectives*, typically relate to the category or categories addressed by the examination and to achieving commitments, specifications, or requirements. Management discloses its principal system objectives in the system description.

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

1.29 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 discussed in paragraph 1.48, the trust services criteria are used to measure the effectiveness of controls in a SOC for Supply Chain examination. 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. Which category or categories are addressed in the description is often determined by considering the commitments the entity makes to its customers and business partners.

1.30 Because of increased dependence on technology and concerns about cybersecurity risks, security is likely to be addressed in most examinations performed using the trust services criteria. Often, customers and business partners of 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.

1.31 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). In that situation, an examination that addresses processing integrity, in addition to security and availability, may best meet the needs of those intended users.

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

1.33 In other situations, the omission of a category that is likely to be important to report users may result in a misleading report. For example, the practitioner may become aware that report users are primarily concerned about cybersecurity risks arising from the interconnection of the entity's system with users' systems. If entity management asked for a report addressing only the availability category, such a report could be misunderstood by users, who would expect the examination to address controls designed, implemented and operated by the entity to mitigate its cybersecurity risks, not only those that threaten the achievement of the entity's availability commitments. In this situation, the practitioner might conclude that an examination addressing only the availability category is likely to be misleading to report users and decide to decline the engagement.

Determining the Time Frame for the Examination

1.34 Paragraph .A1 of AT-C section 105 states that the subject matter of an attestation examination may be "as of a point in time" or "for a 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 guide 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.

Other Engagement Considerations

Considerations for Entities That Distribute Products

1.35 When an entity distributes products, professional judgment is necessary to determine whether the system and controls over the distribution process would be best addressed by the examination described in this guide or by a SOC 2® examination.[16] Perhaps the most important consideration when making this determination is whether the physical distribution of the products is in any way transformative.

1.36 As an example, consider a wholesaler that receives products from multiple manufacturers, assembles the products into surgical kits, and distributes them to hospitals for use in specific types of surgeries. In this example, the wholesaler has transformed those products prior to distribution, and the system controls over the receipt, storage, repackaging, and transportation of the products are likely to have more in common with controls within a manufacturer's system than with controls within a service provider's system. Therefore, in this example, the system that distributes the products would ordinarily be better addressed by a SOC for Supply Chain examination than by a SOC 2® examination. This approach is also more likely to meet the information needs of report users, who are likely to benefit more from SOC for Supply Chain reports from producers, manufacturers, and distribution companies when making decisions related to users' supply chain risk management programs.

1.37 In other situations, a distributor may provide only transportation and delivery of goods produced or manufactured by others or may electronically distribute manufactured software produced by others. In these situations, the system and controls used to provide the distribution services are likely to have more in common with the systems and controls used by a service provider than the systems and controls used to produce or manufacture products. Therefore, a SOC 2® examination may better address the system and controls used to provide the distribution services.

1.38 When making this decision, entity management and the practitioner would carefully consider the facts and circumstances of the engagement, the type of distribution services provided by the entity, the transformative nature of such services, and the information needs of intended users before deciding whether to examine and report on such systems and controls in accordance with the guidance in this guide or in accordance with the guidance for a SOC 2® examination. Appendix B, "Comparison of SOC for Supply Chain, SOC 2®, and SOC for Cybersecurity Examinations and Related Reports," compares certain characteristics of the three examinations and related reports.

Considerations for Entities That Bundle Services With Their Products

1.39 Many entities that produce, manufacture, or distribute products bundle services with the sales of those products. In such situations, it may not

[16] 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 practitioners engaged to examine and opine on a description of a system and related controls of a service provider.

be practical to perform separate examinations of system controls relevant to the production, manufacturing, or distribution of products and system controls used to provide the bundled services. In that case, the responsible party and the practitioner may agree to include the systems and controls within those bundled services within the scope of the SOC for Supply Chain examination.

1.40 When determining whether to include the bundled services within the scope of the examination, practitioners may consider the following examples:

More Likely to Include the Bundled Services in a SOC for Supply Chain Examination	***More Likely to Include the Bundled Services in a SOC 2® Examination***
The services relate to the physical good produced (for example, maintenance services provided in connection with sales of an airplane engine).	The services relate to data or intangible goods produced (for example, health care claims or contract coding).
	The physical good is incidental to the provision of the bundled service. (In this case, a stand-alone report on the service or services may be more useful to intended users.)

Considerations for a Design-Only Examination

1.41 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 over a period of time, entity management makes an assertion only about the suitability of the design of implemented controls as of a point in time. In this guide, such an examination is referred to as a *design-only examination* and includes consideration of the following as of a point in time: (1) whether the description of the entity's system was presented in accordance with the description criteria and (2) whether controls stated in the description were suitably designed and implemented 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 operating effectiveness of controls within the entity's system. Paragraph 4.89 discusses how the practitioner's report presented in table 4-3 could be tailored to refer specifically to the subject matters addressed in a design-only examination.

Matters Not Addressed by a SOC for Supply Chain Examination

1.42 As discussed beginning at paragraph 1.29, an examination described in this guide 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 will meet their product performance specifications.

1.43 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 does not express a conclusion on the products' fitness for purpose or on the merchantability of the products.

Criteria for a SOC for Supply Chain Examination

1.44 The following two types of criteria support the SOC for Supply Chain examination:

a. *Description criteria*. Supplement A of this guide presents an excerpt from 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,*[17] which includes the criteria used to prepare and evaluate the description of the entity's system. The use of these criteria, referred to as the *description criteria*, is discussed further beginning in paragraph 1.45.

b. *Trust services criteria*. Supplement B of this guide presents an excerpt from TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (the 2017 trust services criteria), which includes the criteria used to evaluate the effectiveness of controls relevant to the trust services category or categories included within the scope of a specific examination. The use of these criteria, referred to as the *applicable trust services criteria*, is discussed further beginning in paragraph 1.48.

Description Criteria

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

1.46 The description criteria in supplement A were promulgated by the Assurance Services Executive Committee (ASEC). In establishing and developing these criteria, ASEC followed due process procedures, including exposure

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

of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*,[18] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA council or the board of directors. Paragraph .A44 of AT-C section 105 indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable. Accordingly, these criteria are suitable criteria for preparing and evaluating a description of a system in a SOC for Supply Chain examination. ASEC has also published the description criteria and made them available to users. Therefore, the description criteria meet the requirements in paragraph .25*b*ii of AT-C section 105 for criteria that are both suitable and available for use in an attestation engagement.

1.47 Chapter 3, "Performing the SOC for Supply Chain Examination," discusses how the description criteria are used by the practitioner.

Trust Services Criteria

1.48 The trust services criteria are used to evaluate whether controls were effective to provide reasonable assurance that an entity's principal system objectives were achieved. Because applying the trust services criteria requires judgment, supplement B also presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control — Integrated Framework* (COSO framework) states that points of focus represent important characteristics of the criteria in that framework. Consistent with the COSO framework, the points of focus in supplement B may assist entity management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy. In addition, the points of focus may assist both entity management and the practitioner when evaluating whether controls stated in the description were effective to provide reasonable assurance that the entity's principal system objectives were achieved based on the applicable trust services criteria.

1.49 The trust services criteria in supplement B were promulgated by ASEC. In establishing and developing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA council or the board of directors. Paragraph .A44 of AT-C section 105 indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable. Accordingly, these criteria are suitable criteria for evaluating controls in a SOC for Supply Chain examination. ASEC has also published the trust services criteria and made them available to users. Therefore, the trust services criteria meet the requirements in paragraph .25*b*ii of AT-C section 105 for criteria that are both suitable and available for use in an attestation engagement.

Categories of Trust Services Criteria

1.50 As discussed in paragraph 1.48, the trust services criteria in supplement B are used to evaluate the effectiveness of controls or the design of implemented controls to provide reasonable assurance that the entity's

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

principal system objectives were achieved. 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, or 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 achieve the entity's objectives. (In a SOC for Supply Chain examination, the term *processing integrity* relates to production integrity. In other words, processing is complete, valid, accurate, timely, and authorized to produce, manufacture, or distribute goods that meet the products' 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.

1.51 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.

1.52 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 these 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).

1.53 ASEC has determined that the common criteria are suitable for evaluating the effectiveness of controls to achieve an entity's 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 1-1 identifies the trust services criteria to be addressed when evaluating the effectiveness of controls for each of the trust services categories and indicates how each category is labeled in the table presented in supplement B.

Table 1-1

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)

1.54 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, as discussed beginning at paragraph 1.29.

1.55 Entity management is responsible for evaluating whether controls stated in the description were effective to provide reasonable assurance that the principal system objectives were achieved based on the trust services criteria relevant to one or more of the trust services categories addressed by the examination. Such criteria are referred to throughout this guide as the applicable trust services criteria. For example, in an examination that addresses security, the trust services criteria relevant to security, which are the common criteria (CC1.1–CC9.2) presented in supplement B, are the applicable trust services criteria.

Using the Applicable Trust Services Criteria to Evaluate Control Effectiveness in a SOC for Supply Chain Examination

1.56 As previously discussed, the trust services criteria presented in supplement B are used to evaluate the effectiveness (suitability of design and operating effectiveness) of controls in a SOC for Supply Chain examination. These criteria are based on the COSO framework, which notes that "an organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them." Internal control supports the organization in achieving its objectives. Consequently, to evaluate internal control, the practitioner needs to understand the entity's objectives. For that reason, many of the trust services criteria refer to the achievement of "the entity's objectives."

1.57 In the examination discussed in this guide, the trust services criteria are used to evaluate whether the entity's controls are effective to achieve the entity's system objectives. An entity's system objectives ordinarily refer to the objectives established by entity management for its individual production, manufacturing, or distribution systems. When evaluating whether controls have been designed, implemented, and operated to meet CC3.2, *The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed*, entity management identifies risks to the achievement of its principal system objectives and assesses the likelihood that such risks will be realized as a basis for managing them.

1.58 Chapter 3 discusses in further detail how the practitioner uses the trust services criteria when evaluating whether controls stated in the description were effective to provide reasonable assurance of achieving the entity's principal system objectives based on the applicable trust services criteria.

Evaluating the Entity's Principal System Objectives

1.59 As discussed in paragraph 1.28, an entity's principal system objectives are those that could reasonably be expected to influence relevant decisions made by intended users. Entity management is responsible for identifying the principal system objectives, including the principal commitments made to customers and business partners, the laws and regulations to which the entity is subject, and the industry standards with which the entity needs to comply. 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 management framework issued by the National Institute of Standards and Technology (NIST), the cybersecurity standards issued by the International Organization for 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.

1.60 Table 1-2 illustrates principal system objectives that entity management may identify related to each trust services category addressed by the examination.

Table 1-2

Types of Matters Addressed by Principal System Objectives, Organized 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

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

Trust Services Category	*Matters That Might be Addressed by the Entity's Principal System Objectives*
	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 (which relate to the physical characteristics or functionality of a product)
	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

1.61 Certain commitments an entity makes to customers or business partners may not relate to security, availability, processing integrity, confidentiality, or privacy but may still be relevant to users. For example, dramatic price increases in the cost of raw materials may prevent an entity from delivering goods at contracted prices. The examination described in this guide is not expected to address financial risks such as this.

1.62 Entity management is responsible for designing, implementing, and operating a system and related controls 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 management and the practitioner evaluated the effectiveness of controls. Chapter 2, "Accepting and Planning a SOC for Supply Chain Examination," discusses the principal system objectives in more detail. It also discusses the practitioner's responsibility for assessing whether the principal system objectives disclosed in the description are appropriate.

The Practitioner's Opinion in a SOC for Supply Chain Examination

1.63 At the conclusion of the examination, the practitioner opines on whether (*a*) the description presents the system that was designed and implemented in accordance with the description criteria, in all material respects, 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.

1.64 The practitioner may express an unmodified opinion on the description only if evidence obtained supports a conclusion that the description is free from material misstatement. When considering the materiality of identified misstatements, if any, on the description, the practitioner considers the common information needs of intended users whose decisions are based on the subject matter taken as a whole. Accordingly, it is reasonable for the practitioner to consider whether the description, taken as a whole, is presented in accordance with the description criteria when forming the practitioner's opinion. Although an identified description misstatement that results in the failure to meet one or more description criteria may be indicative of a material misstatement, ultimately the practitioner's opinion focuses on the effect of the misstatement on the description of the system (that is, whether the misstatement could affect decisions made by intended users based on the subject matter taken as a whole).

1.65 The practitioner may issue an unmodified opinion on control effectiveness only if evidence obtained supports a conclusion that controls are effective to provide reasonable assurance that the entity's principal system objectives are achieved. Although one or more control deficiencies may be identified during tests of controls, ultimately, the practitioner's opinion on control effectiveness focuses on the effect of the control deficiencies on the system's ability to provide reasonable assurance that the principal system objectives are achieved, based on the applicable trust services criteria.

Other Types of SOC Examinations: SOC Suite of Services

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

1. SOC 1® — SOC for Service Organizations: ICFR[19]
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

Appendix A, "Information for Entity Management," provides further guidance on each type of service.

Professional Standards

1.67 This guide provides guidance for a practitioner performing a SOC for Supply Chain examination in accordance with the attestation standards. In addition to the performance and reporting guidance in the attestation standards, a practitioner performing such an examination is required to comply with the requirements of other professional standards, such as professional ethics and quality control standards. This section discusses each of the professional standards that apply to the examination.

Attestation Standards

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

1.69 This guide provides additional application guidance to assist a practitioner engaged to perform and report in a SOC for Supply Chain examination. Because this guide is an interpretive publication, paragraph .21 of AT-C section 105 requires the practitioner to consider this guidance when planning and performing such an examination.

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

Code of Professional Conduct

1.71 The AICPA Code of Professional Conduct (code) provides guidance and rules that apply to all members in the performance of their professional

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

responsibilities. The code includes the fundamental principles that govern the performance of all professional services performed by CPAs and, among other things, call for CPAs to maintain high ethical standards and to exercise due care in the performance of all services. When providing attestation services, the "Considering or Subsequent Employment or Association With an Attest Client" subtopic (ET sec. 1.279)[20] of the "Independence Rule" (ET sec. 1.200.001) requires CPAs to be independent in both fact and appearance. Independence in a SOC for Supply Chain examination is discussed further beginning in paragraph 2.16.

Quality in the SOC for Supply Chain Examination

1.72 Paragraphs .06–.07 of AT-C section 105 discuss the relationship between the attestation standards and the AICPA quality control standards. Quality control systems, policies, and procedures are the responsibility of a firm when conducting its attestation practice. Under QC section 10, *A Firm's System of Quality Control*,[21] a CPA firm has an obligation to establish and maintain a system of quality control to provide it with reasonable assurance that

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

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

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

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

Definitions

1.75 Definitions of the terms used in this guide are included in appendix F, "Definitions."

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

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