AICPA

Comparison of SOC for Supply Chain, SOC 2, and SOC for Cybersecurity Examinations and Related Reports

Appendix B

Comparison of SOC for Supply Chain, SOC 2®, and SOC for Cybersecurity Examinations and Related Reports

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

The following table compares a SOC for Supply Chain examination and related report with a SOC 2® examination and a SOC for Cybersecurity examination and related reports. Within the columns, certain text is set in bold to highlight key distinctions between the three types of examinations and related reports.

	SOC for Supply Chain Examination	*SOC 2® Examination*[1]	*SOC for Cybersecurity Examination*[2]
What are the types of organizations for which an examination may be performed?	An entity[3] that produces, manufactures, or distributes products	An organization, or segment of an organization, that provides services to user entities (a service organization)	Any type of organization
Is the examination designed to be performed at a system level or at an entity level?	Generally, the examination is performed on an entity's system or systems that produce, manufacture, or distribute products.	Generally, the examination is performed on a system or systems that provide services.	Generally, the examination is performed on an entity-wide cybersecurity risk management program, although the scope may be narrowed to a specific system, business unit, or function of the entity.
What is the purpose of the report?	To provide specified users (who have sufficient knowledge and understanding of the entity and its system, as discussed later) with information about the controls within the entity's system relevant to security, availability, processing integrity, confidentiality, or privacy to enable users to better understand and manage the risks arising from business relationships with their supplier and distribution networks	To provide specified users (who have sufficient knowledge and understanding of the service organization and its system as discussed later) with information about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy to support users' evaluations of their own systems of internal control	To provide general users with useful information about an entity's cybersecurity risk management program for making informed decisions

	SOC for Supply Chain Examination	*SOC 2® Examination*	*SOC for Cybersecurity Examination*
Who are the intended users?	Entity management and specified parties who have sufficient knowledge and understanding of the entity and its system	Service organization management and specified parties who have sufficient knowledge and understanding of the service organization and its system	Entity management, directors, and a broad range of general users including analysts, investors, and others whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program
Under what professional standards and implementation guidance is the examination performed?	AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*, in AICPA *Professional Standards*	AT-C section 105 and AT-C section 205 in AICPA *Professional Standards*	AT-C section 105 and AT-C section 205 in AICPA *Professional Standards*
	AICPA Guide *SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System*	AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*	AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*
Who is the responsible party?	Entity management	Service organization entity management	Entity management

(continued)

	SOC for Supply Chain Examination	*SOC 2® Examination*	*SOC for Cybersecurity Examination*
Is the report appropriate for general use or is it restricted to specified parties?	Restricted to the use of the entity and specified parties, including the entity's business customers and business partners, accountants providing services to such business customers and business partners, and prospective business customers and business partners who have sufficient knowledge and understanding of 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	Restricted to the use of the service organization and specified parties, such as user entities of the system throughout some or all of the period, business partners subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following: • The nature of the service provided by the service organization • How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties • Internal control and its limitations	Appropriate for general use[4]

	SOC for Supply Chain Examination	*SOC 2® Examination*	*SOC for Cybersecurity Examination*
		• Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements • User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services • The applicable trust services criteria • The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks	

(continued)

	SOC for Supply Chain Examination	*SOC 2® Examination*	*SOC for Cybersecurity Examination*
What is the subject matter of entity management's assertion and the examination?	The description of the entity's production, manufacturing, or distribution system based on the description criteria	The description of the service organization's system based on the description criteria	The description of the entity's cybersecurity risk management program based on the description criteria
	The controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective[5] throughout the period, based on the applicable trust services criteria relevant to security, availability, processing integrity confidentiality, or privacy	Suitability of design and operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to security, availability, processing integrity, confidentiality, or privacy	The effectiveness of controls within that program to achieve the entity's cybersecurity objectives based on the control criteria
What are the criteria for the examination?	The criteria for the description of an entity's system in 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*, in AICPA *Description Criteria*	The criteria for the description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*	The criteria for a description of an entity's cybersecurity risk management program in DC section 100, *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*, in AICPA *Description Criteria*

	SOC for Supply Chain Examination	***SOC 2® Examination***	***SOC for Cybersecurity Examination***
	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria,* contains the criteria for evaluating the effectiveness of controls (*applicable trust services criteria*).	TSP section 100, in AICPA *Trust Services Criteria*, contains the criteria for evaluating the design and operating effectiveness of controls (*applicable trust services criteria*).	The trust services criteria for security, availability, and confidentiality included in TSP section 100, in AICPA *Trust Services Criteria*. Such criteria are suitable for use as control criteria.[6]
What are the contents of the report?	A description of the entity's production, manufacturing, or distribution system A written assertion by entity management about whether (*a*) the description of the entity's system was 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 based on the applicable trust services criteria	A description of the service organization's system A written assertion by service organization management about whether (*a*) the description of the service organization's system was presented in accordance with the description criteria and (*b*) the controls stated in the description were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria	A description of the entity's cybersecurity risk entity management program. A written assertion by entity management about whether (*a*) the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and (*b*) controls within the program were effective in achieving the entity's cybersecurity objectives based on the control criteria

(continued)

	SOC for Supply Chain Examination	*SOC 2® Examination*	*SOC for Cybersecurity Examination*
	A practitioner's report that contains an opinion about whether (*a*) the description of the entity's system was 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 based on the applicable trust services criteria A description of the practitioner's tests of controls and the results of the tests	A service auditor's[7] report that contains an opinion about whether (*a*) the description of the service organization's system was presented in accordance with the description criteria and (*b*) the controls stated in the description were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria A description of the service auditor's tests of controls and the results of the tests	A practitioner's report that contains an opinion about whether (*a*) the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and (*b*) the controls within that program were effective in achieving the entity's cybersecurity objectives based on the control criteria

[1] For illustrative purposes, this table focuses specifically on a type 2 SOC 2® report, which includes both an opinion on the suitability of design and operating effectiveness of controls. AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (SOC 2® guide) provides guidance for service auditors engaged to examine and report on the system that the service organization uses to provide services to user entities and business partners and the controls within the system.

[2] In a SOC 2® examination, when the entity uses the services of a subservice organization, management may elect to use the *inclusive method* or the *carve-out method* to address those services in the description of its system. Those concepts are defined and discussed in the SOC 2® guide.

In the cybersecurity risk management examination, however, entity management is responsible for all controls within the entity's cybersecurity risk management program, regardless of whether those controls are performed by the entity or by a third party. Therefore, the description criteria for use in the cybersecurity risk management examination require the description to address all controls within the entity's cybersecurity risk management program.

[3] If a producer, manufacturer, or distributor bundles the sale of the products with services (for instance, installation), the scope of the SOC for Supply Chain examination may also include those services. There are several factors that are considered when determining whether such services would best be addressed by a SOC for Supply Chain examination or by a SOC 2® examination.

[4] The term *general use* describes reports whose use is not restricted to specified parties. Nevertheless, as discussed in chapter 4 of AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls,* practitioners may decide to restrict the use of their report to specified parties.

[5] Effective controls are those that are both suitably designed and operating effectively.

[6] For both the description criteria and control criteria in a cybersecurity risk management examination, suitable criteria other than those outlined in this appendix may also be used.

[7] The practitioner in a SOC 2® examination is referred to as a *service auditor*.

Appendix C

Illustrative Management Assertion in a SOC for Supply Chain Examination

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

[*ABC Entity's Letterhead*]

Assertion of ABC Entity Management

Introduction

We have prepared the accompanying description of ABC Entity's [*name or type of system*] titled [*insert title of the description*] throughout the period [*date*] to [*date*] (description) based on the criteria for a description of a company's system in 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,* in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the system, including the effectiveness of controls stated therein, that may be helpful when assessing their risks arising from ABC Entity's manufacture and distribution of widgets.

We have also evaluated whether the controls stated in the description, which are necessary to provide reasonable assurance that ABC Entity achieved its principal system objectives, were effective throughout the period [*date*] to [*date*] based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*.[1]

Assertion

We assert that:

- The description presents ABC Entity's system that was designed and implemented throughout the period [*date*] to [*date*] in accordance with the description criteria.
- Based on the evaluation described in the preceding paragraph, the controls stated in the description, which are necessary to provide reasonable assurance that ABC Entity achieved its principal system objectives, were effective throughout the period [*date*] to [*date*], based on the applicable trust services criteria.

---

[1] If there are complementary supplier controls or complementary customer controls that are necessary, in addition to the entity' controls, to provide reasonable assurance that the entity achieves its principal system objectives, entity management may wish to add additional language to the assertion.