APPENDIX A: Comparison of SOC 1®, SOC 2®, and SOC for Cybersecurity Examinations and Related Reports

The following table identifies differences between SOC 1, SOC 2, and SOC for Cybersecurity examinations and related reports. For illustrative purposes, the table focuses specifically on a type 2 SOC report, which includes an opinion on both the suitability of design and the operating effectiveness of controls.

	SOC 1 Examination	***SOC 2 Examination***	***SOC for Cybersecurity Examination***[1]
What are the types of organizations for which an examination may be performed?	An organization, or segment of an organization, that provides services to user entities (a service organization)	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 a system or systems that provide services.	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.
Who is the responsible party?	Service organization management	Service organization management	Entity management

[1] In a SOC 2® examination, when the service organization 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.

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. AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* provides guidance for service auditors engaged to examine and report on an entity's cybersecurity risk management program, including controls within that program.

	SOC 1 Examination	*SOC 2 Examination*	*SOC for Cybersecurity Examination*[1]
What is the subject matter of management's assertion and the examination?	The description of the service organization's system based on the criteria Suitability of design and operating effectiveness of controls stated in the description to achieve the related control objectives stated in the description based on the criteria	The description of the service organization's system based on the description criteria 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 description of the entity's cybersecurity risk management program based on the description criteria 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 and where are they stated?	In AT-C section 320, paragraph .15 contains the minimum criteria for evaluating the description of the service organization's system In AT-C section 320, paragraph .16 contains the criteria for evaluating the suitability of the design of the controls, and paragraph .17 contains the criteria for evaluating the operating effectiveness of the controls.	DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*[2], contains the criteria for evaluating the description of the service organization's system. TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*[3], contains the criteria for evaluating the design and operating effectiveness of the controls.	DC section 100, *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*, in AICPA *Description Criteria,* contains the criteria for evaluating the description of the organization's cybersecurity risk management program. TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022),* contains the trust services criteria for security, availability, and

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

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

	SOC 1 Examination	***SOC 2 Examination***	***SOC for Cybersecurity Examination***[1]
			confidentiality, which are suitable for use as control criteria.[4]
What is the purpose of the report?	To provide service organization management, user entities, and the independent auditors of user entities' financial statements with information and a service auditor's opinion about controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. The report enables the user auditor to perform risk assessment procedures and, if the report is a type 2 report, may provide evidence of the operating effectiveness of controls at the service organization.	To provide service organization management, user entities, business partners, and other specified parties with information and a service auditor's opinion about the system used to provide services and the system controls relevant to security, availability, processing integrity, confidentiality, or privacy.	To provide general users with useful information about an entity's cybersecurity risk management program and the effectiveness of related processes and controls
What are the components of a Type 2 SOC report?	*a.* The description of the service organization's system *b.* A written assertion by management of the service organization about whether, based on the criteria, i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period, in accordance with the criteria	*a.* The description of the service organization's system *b.* A written assertion by management of the service organization about whether i. the description of the service organization's system presents the service organization's system that was designed and implemented throughout the specified period in accordance with the description criteria,	*a.* A description of the entity's cybersecurity risk management program *b.* A written assertion by entity management about whether i. the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and

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

	SOC 1 Examination	***SOC 2 Examination***	***SOC for Cybersecurity Examination***[1]
	ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives, and	ii. the controls stated in the description of the service organization's system were suitably designed throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and	ii. controls within the program were effective in achieving the entity's cybersecurity objectives based on the control criteria
	iii. the controls related to the control objectives stated in management's description of the service organization' system operated effectively throughout the specified period to achieve those control objectives	iii. the controls stated in the description of the service organization's system operated effectively throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria	
	c. A service auditor's report that i. expresses an opinion on the matters in *b*i–*b*iii and ii. includes a description of the service auditor's tests of the controls and the results of those tests	*c.* A service auditor's report that i. expresses an opinion on the matters in *b*i–*b*iii and ii. includes a description of the service auditor's tests of controls and the results of those tests	*c.* A practitioner's report that contains an opinion about whether i. the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and ii. the controls within that program were effective in achieving the entity's cybersecurity objectives based on the control criteria

	SOC 1 Examination	*SOC 2 Examination*	*SOC for Cybersecurity Examination*[1]
Who are the intended users of the report?	Service organization management, user entities during some or all of the period covered by the report (for type 2 reports) and user entities as of a specified date (for type 1 reports), and auditors of the user entities' financial statements	Service organization management and specified parties who have sufficient knowledge and understanding of the service organization's system, including 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 as discussed below.	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
Is the report appropriate for general use or is it restricted to specified parties?	Restricted to the use of specified parties, including service organization management, user entities of the service organization's system, and the independent auditors of such user entities	Restricted to the use of the service organization and other parties who have knowledge of the system; how it interacts with user entities, business partners, subservice organizations, and other parties; the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks; and other matters.	Appropriate for general use[5]

[5] 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.