Illustrative Comparison of the Cybersecurity Risk Management Examination with a SOC 2 Examination and Related Reports

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

The following table compares the cybersecurity risk management examination with a SOC 2 engagement and related reports. Within the Cybersecurity Risk Management Examination and the SOC 2 Engagement columns, certain text is set in bold to highlight key distinctions between the two types of engagement.

	Cybersecurity Risk Management Examination[1]	**SOC 2 Engagement** [2, 3]

[1] In a SOC 2 engagement, 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 its description of its system. Those concepts are defined and discussed in the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 2®)* (the SOC 2 guide).

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

[2] Some of an entity's business partners may need a detailed understanding of controls implemented by the entity and the operating effectiveness of those controls to enable them to design and operate their own control activities. For example, business partners whose IT systems are interconnected with systems at the entity may need to understand the specific logical access protection over the interconnected systems implemented by the entity.

The AICPA Guide, *Reporting on an Entity's Cybersecurity Risk Management Program and Controls,* is not intended to meet the needs of business partners who need a detailed understanding of the entity's specific controls and their operating effectiveness. The SOC 2 guide provides guidance for practitioners engaged to examine and report on system controls at a service organization. In addition, the AICPA intends to develop a vendor supply chain guide to provide guidance for practitioners engaged to examine and report on system controls at a manufacturer or distributer. The vendor supply chain guide is expected to be issued in 2018.

[3] For illustrative purposes, this table focuses specifically on a type 2 SOC 2 report, which includes both an opinion on suitability of design and operating effectiveness of controls.

What is the purpose of the report?	To provide **intended users** with useful information about an entity's cybersecurity risk management program for making informed decisions	To provide a broad range of **system users** 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
Who are the intended users?	Management, directors, analysts, investors, and others whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program	Management of the service organization and other specified parties **with sufficient knowledge and understanding of the service organization and its system**
Under what professional standards and implementation guidance is the engagement 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, *Concepts Common to All Attestation Engagement*s, and AT-C section 205, *Examination Engagements*,[4] in AICPA *Professional Standards*
	The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*	The AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*[5]
Who is the responsible party?	Management of an **entity**	Management of a **service organization**
Is the report appropriate for general use or		**Restricted to user entity personnel and specified parties**, such as independent auditors and practitioners of user entities, prospective user

[4] The clarified attestation standards are effective for practitioner's reports dated on or after May 1, 2017. Prior to that, SOC 2 engagements were performed in accordance with AT section 101, *Attest Engagements* (AICPA, *Professional Standards*).

[5] The AICPA is in the process of updating the SOC 2 guide to incorporate revisions needed to make the guide more responsive to users' cybersecurity concerns. The revised guide is expected to be issued in 2017.

restricted to specified parties?	**Appropriate for general use[6]**	entities, and regulators, who have sufficient knowledge and understanding of the following matters:[7] • The nature of the service provided by the service organization • How the service organization's system interacts with user entities and other parties • Internal control and its limitations • The nature of user entity responsibilities and their role in the user entities' internal control as it relates to service organizations • The nature of subservice organizations and how their services to a service organization may affect user entities • The applicable trust services criteria • The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

[6] The term *general use* refers to reports whose use is not restricted to specified parties. Nevertheless, practitioners may decide to restrict the use of their report to specified parties.

[7] Because the report is only appropriate for users that possess such knowledge and understanding, the SOC 2 report is restricted to the use of such specified users.

What is the subject matter of management's assertion and the engagement?	The description of the **entity's cybersecurity risk management program** based on the description criteria	The description of the **service organization's system** as it relates to one or more of the categories in the trust services criteria
	The effectiveness of controls within that program to achieve the entity's cybersecurity objectives based on the control criteria	Suitability of design and operating effectiveness of controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy based on the criteria
What are the criteria for the engagement?	The **description criteria** included in the AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*	Paragraphs 1.26–1.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* contain the **criteria for the description** of the service organization's system.
	The trust services criteria for security, availability, and confidentiality included in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Such criteria are suitable for use as **control criteria.**[8, 9]	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), contains the **criteria for evaluating the design and operating effectiveness of controls**.

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

[9] The AICPA issued revisions to the extant trust services criteria. The 2017 trust services criteria will be codified as TSP section 100. The extant trust services criteria issued in 2016 will be available in TSP section 100A through December 15, 2018. After that date, the 2016 criteria will be considered superseded. During the transition period

What are the contents of the report?	A description of the **entity's cybersecurity risk management program.** A written assertion by 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 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	A description of the **service organization's system.** A written assertion by management of the service organization regarding the description of the service organization's system and the suitability of the design and the operating effectiveness of the controls in meeting the applicable trust services criteria A service auditor's[10] report that contains an opinion on the fairness of the presentation of the description of the service organization's system and the suitability of the design and operating effectiveness of the controls to meet the criteria **In a type 2 report, a description of the service auditor's tests of controls and the results of the tests**

(April 15, 2017, through December 15, 2018), practitioners should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used.

In addition, the AICPA will continue to make available the 2014 trust services criteria in TSP section 100A-1 until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for practitioner reports for periods ended on or after December 15, 2016.

Because cybersecurity risk management examination engagements are new service offerings, entities that elect to use the trust services criteria as the control criteria in such engagements should use the 2017 revised trust services criteria for security, availability, and confidentiality.

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