Illustrative comparison

of a SOC 2® examination and related report with the cybersecurity risk management examination and related report

Contents

Comparing reports

The following table compares the SOC 2® examination and related report with a cybersecurity risk management examination and related report. Within the SOC 2® examination and the cybersecurity risk management examination columns, certain text is set in bold to highlight key distinctions between the two types of examinations.

	SOC 2® examination[1]	Cybersecurity risk management examination[2,3]
What is the purpose of the report?	To provide **specified users** (who have sufficient knowledge and understanding of the service organization and its system as discussed later in the table) 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
Who are the intended users?	Management of the service organization and specified parties **who have sufficient knowledge and understanding of the service organization and its system**	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, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*,[4] in AICPA *Professional Standards*
	The AICPA Guide SOC 2® *Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*	The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*
Who is the responsible party?	Service organization management	Management of an entity

	SOC 2® examination	Cybersecurity risk management examination[2,3]
Is the report appropriate for general use or restricted to specified parties?	Restricted to the use of the service organization and specified parties, such as user entities of the system throughout some or all 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:[4] • The nature of the service the service organization provides • How the service organization's system interacts with user entities, business partners, subservice organizations and other parties • Internal control and its limitations • 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	Appropriate for general use[5]
What is the subject matter of management's assertion and the examination?	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 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 the cybersecurity risk management program to achieve the entity's cybersecurity objectives, based on the control criteria

	SOC 2® examination	Cybersecurity risk management examination[2,3]
What are the criteria for the examination?	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*[6]	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*
	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*,[7] 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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Such criteria are suitable for use as control criteria*.[8]
What are the contents of the report?	A description of the service organization's system	A description of the entity's cybersecurity risk management program
	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 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 service auditor's[9] 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 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
	In a type 2 report, a description of the service auditor's tests of controls and the results of those tests	

Endnotes

[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.

[2] The 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. 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.

[3] 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.

In the cybersecurity risk management examination, however, 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 service organization. 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.

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

[5] The term *general* use refers to 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.

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

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

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

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

Association
of International
Certified Professional
Accountants®

The unified voice of AICPA and CIMA

P: 888.777.7077 | F: 800.362.5066 | W: aicpa-cima.com