AICPA

SOC 2® examinations and SOC for Cybersecurity examinations:

Understanding the key distinctions

Contents

I. Introduction

In April 2017, the AICPA introduced a new cybersecurity risk management examination (SOC for Cybersecurity) designed to help all types of organizations meet the growing challenge of communicating to interested parties the design and effectiveness of their cybersecurity risk management programs. Since the development of the new SOC for Cybersecurity examination, questions have arisen about the differences between a SOC for Cybersecurity examination and a SOC 2 examination. Although both examinations can provide report users perspective and insight into an organization's cybersecurity controls, there are some meaningful differences between the audience, subject matter, and scope of each that serve a variety of critical marketplace needs. For example, in a SOC for Cybersecurity examination, management of an entity prepares a description of the entity's cybersecurity risk management program and makes an assertion about that description and about the effectiveness of controls within the program, whereas, in a SOC 2 examination, management of a service organization[1] develops a description of a specific system the service organization uses to process transactions for user entities[2] and makes an assertion about that description and about the effectiveness of controls within that system.

This paper describes a SOC for Cybersecurity examination and a SOC 2 examination and addresses the key distinctions between the two examinations.[3]

[1] A service organization is an organization, or segment of an organization, that provides services to user entities.

[2] A user entity is an entity that uses the services provided by a service organization.

[3] 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.

II. Why did the AICPA develop the SOC for Cybersecurity examination?

Filling a marketplace need

Cybersecurity has risen to the top of most organizations' priority lists. Seventy percent of information technology and security professionals believe that cybersecurity threats to their organization are growing, and almost 90 percent have faced at least one attack on their secure systems, according to a 2015 report issued by the Aspen Institute and Intel Security.[4] As boards and managements grapple with the best ways to deal with cyberrisks, they frequently engage information security or cybersecurity consultants to identify problems and potential solutions. These can be valuable services, but they are not designed to offer an independent, entity-wide perspective on an organization's cybersecurity risk management program to the entity's stakeholders.

Seventy percent of information technology and security professionals believe that cybersecurity threats to their organization are growing, and almost **90 percent have faced at least one attack on their secure systems**, according to a 2015 report issued by the Aspen Institute and Intel Security.

With those issues in mind, the AICPA determined that an organization's stakeholders — management, directors, investors, analysts, business partners, and others — would benefit from an independent report on the organization's cybersecurity risk management program, offering useful information they can use to make informed decisions. In response, a Cybersecurity Working Group (working group) of the AICPA Assurance Services Executive Committee (ASEC), in collaboration with the Auditing Standards Board, developed a cybersecurity risk management reporting framework that assists organizations in communicating relevant and useful information about the effectiveness of their cybersecurity risk management programs and CPAs in examining and reporting on the cybersecurity risk management programs. The new framework provides a common and consistent language for organizations to communicate about, and report on, their cybersecurity efforts. The framework has three components:

- **Description criteria.** *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*, for use by management in explaining its cybersecurity risk management programs and by CPAs to report on management's description (SOC for Cybersecurity description criteria)
- **Control criteria.** Criteria for security, availability, and confidentiality included in the 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* for use by CPAs providing advisory or attestation services to evaluate and report on the effectiveness of the controls within the cybersecurity risk management program
- **Attestation guidance.** AICPA Attestation Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* to assist CPAs engaged to examine and report on an entity's cybersecurity risk management program (a SOC for Cybersecurity examination)

This paper focuses on the SOC for Cybersecurity examination, rather than all the elements of the cybersecurity risk management reporting framework, for comparing SOC 2 examinations.

[4] "Critical Infrastructure Readiness Report: Holding the Line Against Cyber Threats." Aspen Institute Homeland Security Program and Intel Security, 2015. https://www.yumpu.com/en/document/view/52187835/rp-aspen-holding-line-cyberthreats/4

III. SOC for Cybersecurity examinations

Purpose, scope and audience

The SOC for Cybersecurity examination is designed to provide report users with information to help them understand management's process for handling enterprise-wide cyberrisks. SOC for Cybersecurity examinations can enhance users' confidence in information prepared by management, enabling them to make informed decisions about the organization and their dealings or transactions with it, and building trust and confidence that management of the entity is appropriately addressing its cybersecurity risks.

The SOC for Cybersecurity examination may be performed for any type of organization, regardless of size or the industry in which it operates. Though the examination has been designed to address an entity-wide cybersecurity risk management program, it may also be performed on any of the following:

a. One or more specific business units, segments, or functions of an entity that operate under an entity-wide cybersecurity risk management program

b. One or more specific business units, segments, or functions of an entity that operate under an independent cybersecurity risk management program

c. One or more specific types of information used by the entity

SOC for Cybersecurity examinations are performed by independent CPAs in accordance with the new AICPA Attestation Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

In a SOC for Cybersecurity examination, an entity's cybersecurity risk management program is defined in the attestation guide as "the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented." Management prepares a description of the cybersecurity risk management program and makes a written assertion about the description and the effectiveness of controls within the program. The CPA examines the information and expresses an opinion on it.

The SOC for Cybersecurity examination report is designed to meet the needs of a broad range of users. Accordingly, it may be appropriate for general use and is not restricted to the use of certain parties. Users might include management and directors who want information about the effectiveness of the entity's cybersecurity controls and investors, analysts, and others whose decisions might be affected by management's process for managing cybersecurity risks.

The SOC for Cybersecurity report includes the following:

1. A description of the entity's cybersecurity risk management program in accordance with the cybersecurity description criteria

2. A written assertion by management about whether (a) the description of the entity's cybersecurity risk management program was presented in accordance with the cybersecurity description criteria and (b) controls within the program were effective in achieving the entity's cybersecurity objectives based on the control criteria

3. A CPA'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 cybersecurity description criteria and (b) controls within the cybersecurity risk management program were effective in achieving the entity's cybersecurity objectives based on the control criteria

Although the CPA's report contains an opinion about the effectiveness of controls within the cybersecurity risk management program, it does not include a description of the detailed tests performed by the CPA and the results of those tests. (As discussed in section IV of this white paper, such information is included in the SOC 2 report.) Instead, the description is included to provide users with the context needed to understand information about the entity's cybersecurity risk management program provided in the report (that is, the evaluation of the effectiveness of the controls within the program).

Hypothetical example: Both ABC Company and DEF Company engage a CPA to perform a SOC for Cybersecurity examination, and the practitioner concludes that both organizations' cybersecurity controls are operating effectively. ABC is a manufacturer of domestic commercial equipment with a mature cybersecurity risk management program that outsources many of its highest-risk IT functions to leading service providers, whereas DEF is a start-up provider of internet-based services to the public, operating worldwide, that changes its systems frequently and has an immature cybersecurity risk management program. Without the information provided in managements' descriptions of each entity's cybersecurity risk management program, a user of both reports lacks the context to understand the differences between their cybersecurity risk management programs.

Another key difference in a SOC for Cybersecurity examination is that management can choose which control criteria are to be used when measuring and evaluating the operating effectiveness of the entity's cybersecurity risk management program, if the criteria meet the definition of suitable criteria under the clarified attestation standards. Management has the option to use as control criteria the AICPA Trust Services Criteria for security, availability, and confidentiality. [A SOC for Cybersecurity examination is not intended to address certain matters related to privacy or processing integrity. For example, a SOC for Cybersecurity examination would address controls over the entity's online prescription ordering systems to maintain the confidentiality of customers' personal health information (PHI), but it would not ordinarily address privacy-specific procedures such as obtaining consent for use of PHI.]

Another **key difference in a SOC for Cybersecurity examination is that management can choose which control criteria are to be used** when measuring and evaluating the operating effectiveness of the entity's cybersecurity risk management program, as long as the criteria meet the definition of suitable criteria under the clarified attestation standards.

IV. SOC 2 examinations

Purpose, scope and audience

SOC 2 examinations are specifically designed to address controls at a service organization relevant to the systems at the service organization used to process users' data. The related report provides users with information needed to understand the effectiveness of controls at the service organization and how they integrate with controls at the user entity. In a SOC 2 examination, service organization management engages the CPA to examine and report on system controls relevant to security, availability, processing integrity, confidentiality, or privacy as set forth in the AICPA's trust services criteria. The scope of the SOC 2 examination may include one or more of these categories, depending upon the circumstances.

Service organization management prepares a description of the system used to process transactions of user entities. The description of the system is prepared using criteria the AICPA developed specifically for that purpose (SOC 2 description criteria). Service organization management also makes an assertion about the description and 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. The CPA examines and expresses an opinion on the description and the controls of the service organization relevant to the applicable trust services criteria.

A SOC 2 report includes the following:

- A description of the service organization's system presented in accordance with the SOC 2 description criteria. The description is designed to provide users with useful information about the service organization's system, including — but not limited to — the types of services provided; the components of the system used to provide them; the boundaries of the system; and the controls service organization management has designed, implemented, and operated to achieve its service commitments and system requirements based on the applicable trust services criteria.
- A written assertion by the service organization's management that addresses whether the description of the service organization's system is presented in accordance with the SOC 2 description criteria and 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 service auditor's opinion about whether the description of the service organization's system was presented in accordance with the SOC 2 description criteria and 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 detailed description of the service auditor's tests of controls and results thereof.

In contrast to a SOC for Cybersecurity examination, in which management may select the criteria against which to evaluate the effectiveness of controls to achieve the entity's cybersecurity objectives, a SOC 2 examination may only be performed using the AICPA trust services criteria.

SOC 2 examinations are performed by independent CPAs in accordance with 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).[5]

[5] The AICPA is in the process of updating the extant guide (2015 version) to (1) align the guidance to requirements of the clarified attestation standards under which the examination is performed, (2) address the revised description criteria to be issued by ASEC first quarter of 2018), (3) address the revised trust services criteria issued by ASEC in April 2017, and (4) incorporate, as appropriate, new concepts included in (a) AICPA Guide Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SOC 1®), and (b) AICPA Attestation Guide Reporting on an Entity's Cybersecurity Risk Management Program and Controls. This paper uses guidance from the updated SOC 2 guide that is expected to be issued first quarter of 2018.

SOC 2 reports help service organizations foster trust and confidence in their service delivery processes and controls. Stakeholders who use these reports include user entities, business partners, and CPAs providing services to such user entities and business partners who want to assess and manage risks associated with outsourcing a function to a service organization.

As previously stated, SOC 2 reports include details of the controls the CPA tested and the results of those tests, which can be very valuable to report users. Because of this detailed information included in SOC 2 reports, SOC 2 reports are restricted to user entity personnel and specified parties 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
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with 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

Although not the primary users of SOC 2 reports, boards also may find SOC 2 reports helpful in fulfilling their organizational oversight responsibilities, including oversight of vendor management programs, risk management processes, and regulatory compliance matters.

SOC 2 reports help service organizations **foster trust and confidence in their service delivery processes and controls**.

Hypothetical example: XYZ Company is a diverse multinational services company. One of XYZ Company's divisions is its Fictional Cloud Services (FCS) division, which provides infrastructure as a service (IaaS) to a growing group of customers. FCS commissions a CPA to examine and report on controls over the security and availability of its IaaS system over a one-year period.

The SOC 2 examination addresses only the system or systems used to provide IaaS and the controls relevant to security and availability. It would not extend to other services or products the FCS division or its parent, XYZ Company provided. In contrast, XYZ Company could engage the CPA to perform a SOC for Cybersecurity examination over the FCS's cybersecurity risk management program, which would include controls relevant to security and availability within that program.

Though the SOC 2 report is intended only for the use of FCS and current and prospective users of its services who have a sufficient level of understanding of the service organization and its IaaS system to understand the report, the SOC for Cybersecurity report would be appropriate for general users.

V. Summary comparison of SOC for Cybersecurity examinations and SOC 2 examinations

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

	SOC for Cybersecurity examination[6]	SOC 2 examination[7]
What is the purpose of the report?	To provide **general users** with useful information about an entity's cybersecurity risk management program for making informed decisions	To provide **specified users** (who have sufficient knowledge and understanding of the service organization and its system as discussed here) 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, 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	Management of the service organization and specified parties **who have sufficient knowledge and understanding of the service organization and its system**
Who can perform the examination and under what professional standards and implementation guidance is the examination performed?	Independent CPAs under AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*) AICPA Attestation Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*	Independent CPAs under AT-C section 105, *Concepts Common to All Attestation Engagements, and AT-C section 205, Examination Engagements* (AICPA, *Professional Standards*) *AICPA Guide SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, processing integrity, confidentiality, or privacy*[8]

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

[7] In a SOC for Cybersecurity 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 for use in the SOC for Cybersecurity examination require the description to address all controls within the entity's cybersecurity risk management program.

[8] The AICPA is in the process of updating the 2015 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 first quarter of 2018.

	SOC for Cybersecurity examination[6]	SOC 2 examination[7]
Who is the responsible party?	Management of an **entity**	**Service organization** management
Is the report appropriate for general use or restricted to specified parties?	**Appropriate for general use**[9]	**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 user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:[10] • 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 • 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 service • 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

[9] 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.

[10] 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.

	SOC for Cybersecurity examination[6]	SOC 2 examination[7]
What is the subject matter of management's assertion and the examination?	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	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
What are the criteria for the examination?	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 (AICPA, Description 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 (AICPA, Trust Services Criteria). Such criteria are suitable for use as **control criteria**.[11]	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® 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 (applicable trust services criteria).**

[11] For both the description criteria and control criteria in a SOC for Cybersecurity examination, suitable criteria other than those outlined in this table may also be used.

	SOC for Cybersecurity examination[6]	SOC 2 examination[7]
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 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 service auditor's[12] 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 **In a type 2 report, a description of the service auditor's tests of controls and the results of the tests**

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