Frequently asked questions

Effect of the use of software tools on SOC 2® examinations

As of June 30, 2021

About the Association

The Association of International Certified Professional Accountants® (the Association) is the most influential body of professional accountants, combining the strengths of the American Institute of CPAs® (AICPA®) and The Chartered Institute of Management Accountants® (CIMA®) to power trust, opportunity and prosperity for people, businesses and economies worldwide. It represents 650,000 members and students in public and management accounting and advocates for the public interest and business sustainability on current and emerging issues. With broad reach, rigor and resources, the Association advances the reputation, employability and quality of CPAs, CGMA® designation holders and accounting and finance professionals globally.

Notice to readers

These frequently asked questions (FAQs) were prepared by AICPA staff to provide nonauthoritative guidance on selected practice matters raised by members in connection with SOC 2® examinations. These FAQs represent the views of AICPA staff based on the input of members of the SOC 2 Working Group; they have not been approved, disapproved or otherwise acted upon by any senior committee of the AICPA.

The relevant attestation standards, including AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*,[1] contain performance and reporting requirements and application guidance for examination engagements.[2] Furthermore, 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) provides additional application guidance for SOC 2 examinations.

[1] In September 2020, the AICPA Auditing Standards Board (ASB) issued Statement on Standards for Attestation Engagements (SSAE) No. 21, Direct Examinations. SSAE No. 21 supersedes extant AT-C section 205 and changes the title of that section from *Examination Engagements to Assertion-Based Examination Engagements* to differentiate it from the newly created AT-C section 206, *Direct Examination Engagements*. SSAE No. 21 is effective for reports issued on or after June 15, 2022.

[2] All AT-C sections can be found in AICPA *Professional Standards*.

Introduction

In recent years, a number of software solutions (herein referred to as SOC 2 tools or tools) have been introduced that are designed to improve the efficiency with which service organizations can prepare for and undergo SOC 2 examinations.[3] Such tools may be hosted on the service organization's system or provided as software-as-a-service (SaaS) solutions.

A SOC 2 tool can sometimes be similar to a governance, risk management and compliance (GRC) tool. Such tools may enhance efficiency by collecting and organizing a service organization's SOC 2 documentation in a central repository or integrated data connections. The service auditor can access that information to support the understanding of the design of the service organization's controls; this understanding then serves as a basis for the auditor's design of procedures to obtain evidence about the suitability of the design and operating effectiveness of the service organization's controls. In other situations, a SOC 2 tool's functionality may enable service organization management to perform risk assessment, vendor management or control monitoring. In such circumstances, the provider of the SOC 2 tool (hereafter referred to as the *SOC 2 tool provider or tool provider*) may be considered a subservice organization. Furthermore, in some cases the tools can be considered part of the service organization's system of internal control.

SOC 2 tools that are properly designed, configured and managed may benefit both service organization management and service auditors. Depending on the scope and functionality of such tools and how service organizations use them, however, risks can arise that service auditors should be aware of when performing a SOC 2 examination.

The objectives of these FAQs are as follows:

- Describe risks that arise from the functionality of SOC 2 tools and the service organization's use of such tools.
- Remind service auditors that a service organization's use of a SOC 2 tool does not change the service auditor's responsibilities to comply with relevant professional standards.
- Highlight specific requirements of the standards and certain independence considerations that may be relevant when a service organization uses a SOC 2 tool.
- Discuss how certain business relationships between service auditors and SOC 2 tool providers can threaten service auditor's compliance with professional and ethical responsibilities.

[3] Although similar tools may be marketed to organizations engaging a CPA to perform other attestation engagements, this document addresses only the potential impact of the use of such tools on SOC 2 examinations. Nevertheless, some of the guidance may be helpful when considering the effect of similar tools in other attestation engagements.

Inquiry. In relation to a SOC 2 examination, what risks arise from a service organization's use of a SOC 2 tool?

Reply. Such risks are based on the scope and functionality of a SOC 2 tool and on how the service organization uses it; these risks include the following (this is not intended to be a comprehensive list):

- **The tool does not function as intended.** A SOC 2 tool that does not function as intended could result in the service organization furnishing the service auditor with incorrect information; this in turn could result in an erroneous opinion in the SOC 2 examination. For example, if a SOC 2 tool collects technical configuration data from the service organization's separate system-event log and operational monitoring tools, but the application programming interface that connects these systems does not operate correctly, the SOC 2 tool might receive incomplete or inaccurate information.

- **Service organization management does not adequately understand the effect of services provided by the tool provider on its system of internal control.** Depending on the scope and functionality of a SOC 2 tool and how it is used by the service organization, the tool provider could be a subservice organization, or those services could be considered part of the service organization's system of internal control. Because the use of such tools by service organizations is relatively new, there is a risk that service organization management will fail to fully understand the implications of their use on the system of internal control. Management could rely too heavily on a SOC 2 tool and related services or management could fail to use the tool and related services correctly. For example, if a service organization's system uses unique technologies not contemplated by the tool's risk assessment functionality — and management were to perform risk assessment *by use of that functionality alone* — the risk assessment could be incorrect or incomplete. As a result, controls might not be suitably designed or operating effectively to address the risks that arise from the use of such unique technologies.

- **Service organization management lacks the skills and competencies to properly use the SOC 2 tool and related tool-provider services.** Such a lack of skills and competencies could, for instance, cause management to rely too heavily on the tool's risk assessment function, its list of common controls, or its library of policies and procedures when management undertakes to design and implement effective controls to provide reasonable assurance that the service organization achieves its service commitments and system requirements based on the applicable trust services criteria (TSC). In such circumstances, management may be unable to accept responsibility for the suitability of the design and — in a type 2 examination — the operating effectiveness of controls to provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable TSC.[4] In addition, management (the responsible party) may not have a reasonable basis for measuring or evaluating the subject matter on which it bases its assertion.[5]

[4] Paragraph 2.43 of 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) states that the service auditor should accept or continue an engagement only when the preconditions for an attestation engagement identified in paragraphs .24 and .25 of AT-C section 105, *Concepts Common to All Attestation Engagements*, are met; one of those preconditions is that management will be able to take responsibility for the subject matter of the engagement.

[5] Paragraph 2.45 of the SOC 2 guide indicates that, as one of the preconditions of the SOC 2 examination, the service auditor should determine whether the subject matter is appropriate for the engagement. According to paragraph .A36 of AT-C section 105, one element of the appropriateness of the subject matter is the existence of a reasonable basis for its measurement or evaluation. Without a reasonable basis for measuring or evaluating the subject matter, the subject matter would not be appropriate; therefore, management would not be able to provide the service auditor with a written assertion as required by the SOC 2 guide. Paragraphs 2.49–.56 of the SOC 2 guide discuss this issue in further detail.

Inquiry. How might a service organization's use of a SOC 2 tool (or services of the tool provider) affect how the service auditor meets relevant responsibilities in a SOC 2 examination?

Reply. A service auditor is responsible for performing a SOC 2 examination in accordance with the requirements in both AT-C section 105 and AT-C section 205. The SOC 2 guide is an interpretive publication that provides recommendations on the application of those standards when planning and performing a SOC 2 engagement.

Chapter 2 of the SOC 2 guide discusses the service auditor's responsibilities in a SOC 2 examination. Although a service organization's use of a SOC 2 tool does not change the responsibilities of the service auditor as outlined in the SOC 2 guide, it might affect how the service auditor *meets* those responsibilities.

The table that follows provides examples of how a service organization's use of a SOC 2 tool might affect how the service auditor meets relevant requirements of the attestation standards. The table is not intended to present all of the ways in which SOC 2 tools may be used, nor how such use could affect every responsibility of the service auditor in a SOC 2 examination.

Examples of Service Organization's Use of a SOC 2 Tool	Resulting Considerations for the Service Auditor
Management uses a SOC 2 tool's predefined list of common controls to design and implement system controls without tailoring the controls to the service organization's system.	Service organization management is responsible for the following: • Identifying and assessing risks that threaten the achievement of the service organization's service commitments and system requirements based on the TSC • Designing, implementing, operating, monitoring and documenting controls that are suitably designed and, in a type 2 examination, operating effectively to mitigate such risks and provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable TSC When designing controls that mitigate assessed risks, management may not be able to rely solely on predefined or standardized control listings embedded in a SOC 2 tool because such controls may fail to address risks that are unique to the service organization. For example, a SOC 2 tool may recommend, in a predefined list of common controls, that the service organization perform a vulnerability scan at least quarterly. However, performing such scans on a quarterly basis may not be often enough for a service organization that provides services in an industry vulnerable to data breaches, ransomware attacks and other intrusions. Management's misuse of or overreliance on a tool's predefined listing of controls could fail to identify and assess all relevant risks; this is likely to result in deficiencies in the design of implemented controls and could lead to a modification of the service auditor's opinion on both the description of the system and the suitability of design of controls.

Examples of Service Organization's Use of a SOC 2 Tool	Resulting Considerations for the Service Auditor
Management uses a SOC 2 tool to aggregate documentation for the service auditor that demonstrates the suitability of the design and operating effectiveness of controls to provide reasonable assurance of achieving the service organization's service commitments and system requirements.	Information generated by a SOC 2 tool is considered information provided by the entity (IPE). Therefore, regardless of the tool's functionality, management is expected to have evaluated the accuracy and completeness of the information produced or maintained by the tool before incorporating that information into its system and its system description. Management may have evaluated one or more of those matters in the following ways: • Performing its review of the information aggregated by the SOC 2 tool to determine its reliability and relevance to the SOC 2 examination • Performing its tests of controls related to the SOC 2 tool • Obtaining and reviewing a practitioner's attestation report, such as a SOC 2 report on processing integrity on a SOC 2 tool or a SOC for Supply Chain report on processing integrity over the process used in developing the SOC 2 tool (Before relying on such a report, though, management needs to consider whether and how the controls addressed in the report apply to the service organization's system.) The service auditor's responsibility to obtain sufficient appropriate evidence throughout the engagement to support the service auditor's opinion is unchanged by management's use of a SOC 2 tool. When using IPE in a SOC 2 examination, the service auditor is required by paragraph .35 of AT-C section 205 to evaluate whether the information is sufficiently reliable for the service auditor's purposes. The service auditor may need to perform procedures to determine whether the tool functions as intended and that the information generated by the tool is reliable for the service auditor's purposes. This may be done as follows: a. Obtaining evidence about the accuracy and completeness of the information (If management has obtained a practitioner's attestation report on the tool, reviewing that report may assist the service auditor in making that evaluation.) b. Evaluating whether the information is sufficiently precise and detailed for the service auditor's purposes As previously discussed, a SOC 2 report on processing integrity of the SOC 2 tool or a SOC for Supply Chain report on processing integrity over the process used in developing the SOC 2 tool might help the service auditor evaluate the functionality of the SOC 2 tool. Once the service auditor has determined that the information generated by the tool is sufficiently reliable for the service auditor's purposes, the service auditor may use such information when performing procedures to obtain sufficient appropriate evidence about whether controls are suitably designed and, in a type 2 examination, operating effectively to provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable TSC.

Examples of Service Organization's Use of a SOC 2 Tool	Resulting Considerations for the Service Auditor
Management uses a SOC 2 tool and related services provided by a tool provider.	In obtaining an understanding of the service organization's system and system controls described in the description of the system, the service auditor is required to obtain an understanding of the processes and controls performed by a SOC 2 tool. In addition to its responsibility for ongoing monitoring activities, management is responsible for determining whether the SOC 2 tool provider is a subservice organization, as discussed in paragraphs 2.06–.11 of the SOC 2 guide. If management determines that the tool provider is a subservice organization, management is also responsible for the following: • Determining the method (inclusive or carve-out) that will be used to describe the services provided by the SOC 2 tool provider in the description of the system • Identifying and assessing any risks of doing business with the subservice organization • Designing, implementing, and operating controls to mitigate those risks • Monitoring the services and controls performed by the subservice organization Again, a SOC 2 report on processing integrity of the SOC 2 tool or a SOC for Supply Chain report on processing integrity over the process used in developing the SOC 2 tool may help the service auditor evaluate the functionality of the SOC 2 tool. Paragraphs 2.12–.16 of the SOC 2 guide further detail those responsibilities. If service organization management elects to use the inclusive method and the SOC 2 tool provider agrees to be a responsible party in the SOC 2 examination, the tool provider is considered a subservice organization; subservice organization management has many of the same responsibilities as service organization management (see paragraph 2.101 of the SOC 2 guide). Furthermore, because the tool provider is a responsible party, the service auditor should be independent of the tool provider. Independence is addressed in the subsequent Q&A.

Inquiry. The AICPA Code of Professional Conduct (the code) applies to all members in the performance of their professional responsibilities. It includes the fundamental principles that govern the performance of all professional services performed by CPAs and, among other things, calls for CPAs to maintain high ethical standards and to exercise due care in the performance of all services.

When independence is required by relevant professional standards, the code provides guidance on determining whether a member is independent. Are there circumstances in which a service organization's use of a SOC 2 tool may present threats to a service auditor's independence?

Reply. Yes. As noted earlier, if the SOC 2 tool provider is (1) determined to be a subservice organization and (2) service organization management, in the description of the system, elects to use the inclusive method to disclose the services provided by the subservice organization, subservice organization management is also a responsible party in the SOC 2 examination. In this situation, paragraph 2.37 of the SOC 2 guide states that the service auditor is also required to be independent of the subservice organization.

Inquiry. A service auditor may enter into a business relationship with a SOC 2 tool provider whose tool is used by one or more of the service auditor's SOC 2 clients. Are there situations in which certain business relationships create threats to the member's ability to comply with other ethical rules of the code?

Reply. Yes. Depending on the nature of the relationship between the service auditor and a SOC 2 tool provider, threats to the member's ability to comply with independence rules (and other rules) in the code may arise.

The table that follows presents certain relationships and their related risks. The table neither intends to present all possible business relationships nor to identify all potential threats to a service auditor's ability to meet ethical requirements under the code.

Examples of business relationships between a Service Auditor and a SOC 2 Tool Provider	Ethics Guidance or Rulings to consider
On its website or through other media, the SOC 2 tool provider promotes the service auditor's SOC 2 services (with the service auditor's consent and with or without the service auditor paying the SOC 2 tool provider a referral fee) to service organizations and promises a discount on the service auditor's fees if the service auditor is engaged to perform the examination.	The "Integrity and Objectivity Rule" The member should consider whether he or she is in compliance with the "Integrity and Objectivity Rule" (ET sec. 1.100.001),[6] which states that "in the performance of any professional service, a member shall maintain objectivity and integrity, shall be free of conflicts of interest, and shall not knowingly misrepresent facts or subordinate his or her judgment to others." The "Conflicts of Interest for Members in Public Practice" interpretation (ET sec. 1.110.010) of that rule states in part that [a] member or his or her firm may be faced with a conflict of interest when performing a professional service. In determining whether a professional service, relationship, or matter would result in a conflict of interest, a member should use professional judgment, taking into account whether a reasonable and informed third party who is aware of the relevant information would conclude that a conflict of interest exists. The interpretation provides examples of conflicts of interest and guidance on how to identify business relationships that might create a conflict of interest, as well as guidance on how to evaluate whether the significance of the threat it poses is at an acceptable level.

[6] All ET sections can be found in AICPA *Professional Standards*.

Examples of business relationships between a Service Auditor and a SOC 2 Tool Provider	Ethics Guidance or Rulings to consider
	The "Advertising and Other Forms of Solicitation Rule" The "Advertising and Other Forms of Solicitation Rule" (ET sec. 1.600.001) states that "a member in public practice shall not seek to obtain clients by advertising or other forms of solicitation in a manner that is false, misleading, or deceptive. Solicitation by the use of coercion, over-reaching, or harassing conduct is prohibited." The "False, Misleading, or Deceptive Acts in Advertising or Solicitations" interpretation (ET sec. 1.600.0100) states in part that > [a] member would be in violation of that rule if the member's promotional efforts are false, misleading, or deceptive. If a member is asked to perform professional services for a client or customer of a third party, the member should determine that the third party's promotional efforts comply with the "Advertising and Other Forms of Solicitation Rule." Such action is required because the member will receive the benefits of such efforts by third parties, and members must not do through others what they are prohibited from doing themselves. Accordingly, if the member plans to enter into a relationship like this with a SOC 2 tool provider, the member may want to ensure that the promotional efforts of the SOC 2 tool provider are aligned with the rule. For example, if the member does not plan to discount the fee for clients that use the SOC 2 tool, the promotion by the tool provider could be viewed as being false, misleading, or deceptive. The "Commissions and Referral Fees Rule" The "Commissions and Referral Fees Rule" (ET sec. 1.520.001) states, with respect to referral fees, that "any member who accepts a referral fee for recommending or referring any service of a CPA to any person or entity or who pays a referral fee to obtain a client shall disclose such acceptance or payment to the client." The "Disclosure of Commissions and Referral Fees" interpretation (ET sec. 1.520.080) of that rule requires the disclosure to be in writing. Accordingly, if a member pays a SOC 2 tool provider for referring its users to the member to provide a SOC 2 examination, the member should disclose the referral fee in writing to the new client.

Examples of business relationships between a Service Auditor and a SOC 2 Tool Provider	Ethics Guidance or Rulings to consider
The SOC 2 tool provider and the service auditor enter into a relationship; the service auditor decides to rely solely on the SOC 2 tool to generate all audit evidence and other information necessary to support the service auditor's opinion, enabling the service auditor to merely sign the SOC 2 report generated by the tool.	The "Compliance With Standards Rule" The "Compliance With Standards Rule" (ET sec. 1.310.001) states that a member that performs auditing, review, compilation, management consulting, tax, or other professional services, shall comply with standards promulgated by bodies designated by the AICPA Council. It would not be appropriate for a service auditor to sign the service auditor's report unless he or she has complied with all applicable standards. As discussed in the first Q&A, a service auditor's responsibilities in a SOC 2 examination do not change solely because the service organization uses a SOC 2 tool. The service auditor is responsible for complying with the relevant attestation standards in AT-C sections 105 and 205; the service auditor also has a responsibility to consider applicable interpretive guidance in the SOC 2 guide. For example, according to paragraph 2.30 of the SOC 2 guide, the service auditor is responsible for a. determining whether all preconditions are met before accepting the engagement; b. obtaining an understanding of the service organization's system and controls, including that of the SOC 2 tool provider if it is considered to be a subservice organization and management has elected to use the inclusive method; c. performing an independent risk assessment to identify and assess risks to the service organization's achievement of its service commitments and system requirements based on the applicable TSC; d. designing and performing procedures that are responsive to those risks; e. obtaining sufficient appropriate evidence about the effectiveness of controls to support the opinion; and f. issuing an appropriate SOC 2 report containing that opinion. None of those responsibilities are eliminated because a SOC 2 tool is used by the service organization, regardless of how it is used.

P: 919.402.4500 | F: 919.402.4505 | W: aicpa.org

Brought to you by the Association of International Certified Professional Accountants, the global voice of the accounting and finance profession, founded by the American Institute of CPAs and The Chartered Institute of Management Accountants.