November 2020

Frequently asked questions

SOC 2® and SOC 3® examinations

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® and SOC 3® examinations. These FAQs represent the views of AICPA staff based on the input of members of the AICPA Assurance Services Executive Committee's 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*, contain performance and reporting requirements and application guidance for examination engagements.[1,2] Service auditors who perform SOC 2 and SOC 3 examinations are required to comply with those requirements. Furthermore, 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) provides additional application guidance for SOC 2 and SOC 3 examinations.

[1] All AT-C sections can be found in AICPA Professional Standards. www.aicpa.org/research/standards/auditattest/ssae.html

[2] A SOC 2 examination may also be performed in accordance with AT Section 101, *Attest Engagements*, of the PCAOB's interim attestation standards.

.01 CHANGE IN THE OPINION ON DESIGN AND OPERATING EFFECTIVENESS

Inquiry—Prior to the 2017 revisions to the trust services criteria and the corresponding changes to the SOC 2 guide (January 2018), the service auditor formed the opinion on design and operating effectiveness in a SOC 2 examination by considering whether an identified control deficiency resulted in the service organization's failure to meet one of more of applicable trust services criteria. After such revisions were made, however, the service auditor formed the opinion by considering the effect of any identified control deficiencies on the service organization's *ability to meet its service commitments and system requirements based on the trust services criteria.* Why did the service auditor's opinion on design and operating effectiveness change, and how does the change affect a service auditor's opinion on the design and operating effectiveness of controls in a SOC 2 examination?

Reply—The reason for the change in the opinion relates primarily to the 2017 revisions to the trust services criteria. The trust services criteria were revised to conform to the 2013 COSO framework,[3] which notes that "an organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them." Internal control supports the organization in achieving its objectives. Consequently, for report users to understand how the effectiveness of controls within a system are evaluated in a SOC 2 examination, they need to understand the objectives that management has established for the system. For that reason, management also discloses the principal[4] objectives in the description of the system; in the description, those objectives are referred to collectively as the service organization's *service commitments* and *system requirements.*

Management derives the service organization's principal service commitments and system requirements from the following:

a. The *service commitments* it makes to user entities related to the system used to provide the services
b. The *system requirements* necessary to achieve those commitments
c. The need to comply with laws and regulations regarding the provision of the services by the system
d. Other objectives service organization management has for the system

Prior to the revisions to the trust services criteria and guide, the auditor's opinion implied that the design and operating effectiveness of controls were evaluated by considering only whether the applicable trust services criteria were met. The change in the service auditor's opinion, though subtle, clarifies that the service auditor's opinion on design and operating effectiveness of system controls depends on whether those controls were effective to provide reasonable assurance that the overall system objectives (that is, the *service commitments* and *system requirements*) were achieved; the trust services criteria are the framework against which that evaluation is made.

---

[3] Committee of Sponsoring Organizations (COSO). Internal Control –Integrated Framework. May 2013. www.coso.org/Pages/ic.aspx

[4] The SOC 2 guide defines the *principal* service commitments and system requirements as those common to the majority of user entities. Disclosure in the description of the system of a service organization's principal service commitments and system requirements is necessary to enable report users to understand how the system operates and how management and the service auditor evaluated the suitability of the design of controls and, in a type 2 examination, the operating effectiveness of controls.

Inquiry—Are there situations in which the same control deficiency identified during the SOC 2 examinations of two different service organizations may lead the service auditor to issue a qualified opinion on operating effectiveness for one service organization but not for the other?

Reply—Yes. When a control deficiency is identified, the service auditor is responsible for evaluating the effect of the deficiency by considering the effect on the system's ability to achieve the service commitments and system requirements that management established based on the trust services criteria. Although the same identified control deficiency may have resulted from the evaluation of a particular trust services criterion, the effect of the deficiency on the overall effectiveness of the system and related controls (that is, whether controls provide reasonable assurance of achieving the service organization's service commitments and system requirements) may be different at each organization.

Decisions about the effect of control deficiencies identified during the examination are very complex and involve a high degree of professional judgment; consequently, the same deficiency may result in a different conclusion based on the particular facts and circumstances. Let's look at a simple example that illustrates this response. Assume that service organizations A and B provide cloud infrastructure-as-a-service to commercial entities; both organizations provide failover processing through load balancing across geographically diverse data centers. The service auditor's testing reveals that in both organizations the design of the failover processing results in a likelihood that processing capacity will be 50% of peak load for the first day of failover due to system resource limitations and the process for reallocating resources. Company A's target market is SaaS entities that provide storage and retrieval of services, and its service commitment around availability is based on monthly total capacity available. Company B's target market is companies that provide financial instrument trading platforms, and its service commitment around availability is based on peak transaction processing volume. In this example, a service auditor of the two organizations is likely to reach different conclusions when evaluating the effect of the deficiency on the achievement of the organizations' availability commitments.

.02 TRUST SERVICES CATEGORIES ADDRESSED

Inquiry—How does service organization management determine which trust services categories to include within the scope of the SOC 2 examination? What is the service auditor's responsibility for determining whether those categories are appropriate for the examination?

Reply—Service organization management is responsible for selecting the trust services category or categories to be included within the scope of the examination based on its understanding of the needs of user entities and what it wants to communicate to those user entities.

Because service organizations and their customers and business partners

have an increased dependence on technology, including concerns about cybersecurity risks and their impact on operational processes, security controls are a primary area of focus for system users. As a result, for most service organizations, management will include the security category within the scope of the examination. When determining other categories to include and address in the examination, service organization management usually considers the commitments it makes to its customers and business partners, as in the following examples:

- A service organization that provides IT infrastructure services to its customers and business partners may have made certain commitments to its customers and business partners about security and system availability; therefore, a SOC 2 examination that addresses the security and availability categories is likely to meet its customer and business partner informational needs.

- A service organization that processes proprietary information or personal information for its customers and business partners may make commitments about maintaining the confidentiality or privacy of the information processed. In this case, a SOC 2 examination that addresses security and the confidentiality or privacy categories may meet users' needs.[5]

According to paragraph 2.46 of the SOC 2 guide, when evaluating the appropriateness of the subject matter, a service auditor may consider the relevance of a trust services category or categories included within the scope of the examination to the system. If the service auditor believes the omission of a category that may be relevant to intended users' understanding of the system increases the risk that users will misunderstand the service auditor's opinion in the SOC 2 report, the service auditor may discuss the concern with service organization management. For example, if management discloses in the description of the system a principal service commitment around the availability of the system to its customers, such customers are likely to expect the availability category to be included within the scope of the SOC 2 examination. In this situation, if service organization management is unwilling to include the availability category within the scope of the examination or exclude the availability related commitment from the description, the service auditor may decide to decline the engagement.

Inquiry—As discussed in the prior response, the security category is included in the majority of SOC 2 examinations. Are there circumstances in which a service auditor may accept a SOC 2 examination that excludes the security category from the scope of the examination?

Reply—Yes, management may determine that a report omitting the security category meets the needs of intended users of the report. Paragraph 1.38 of the SOC 2 guide states that, even if the SOC 2 examination is only on availability, the controls examined should include **all the common criteria** in addition to the specific criteria for availability. That is important because a control deficiency in a control necessary to meet the common criteria may affect the service organization's ability to achieve its service commitments and system requirements. Therefore, the service auditor still has to evaluate the suitability of design and, in a type 2 examination, the operating effectiveness of controls necessary to meet all of the common criteria (CC1.1 through CC9.2), which encompass controls such as those over

[5] Paragraphs 1.25 and 1.26 of the SOC 2 guide discuss the difference between the confidentiality and privacy categories.

logical and physical access controls, systems operations, and change management in addition to controls necessary to meet the criteria related to the availability category.

.03 COMMON CONTROLS TO MEET THE TRUST SERVICES CRITERIA

Inquiry—Is there a minimum set of controls or standardized template of controls that organizations can implement to help ensure that controls are suitably designed based on the applicable trust services criteria in a SOC 2 examination?

Reply—No, there is no minimum set of controls or standardized template of controls that help ensure controls are suitably designed to meet the applicable trust services criteria. A service organization should implement specific controls designed to mitigate risks identified by management, which could prevent the service organization from achieving its service commitments and system requirements. For that reason, the trust services criteria do not prescribe specific controls for any organization. Instead, the trust services criteria establish the outcomes that those controls should meet to achieve a service organization's service commitments and system requirements.

.04 SOC PROVIDERS

Inquiry—Who can perform a SOC 2 examination?

Reply—In the United States, a SOC 2 examination is performed by a licensed CPA in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements,* and AT-C section 205, *Examination Engagements*, of the attestation standards established by the AICPA and the SOC 2 guide.

The publication *Performing and Reporting on a SOC 2® Examination in Accordance with International Standards on Assurance Engagements (ISAEs) or in Accordance with Both the AICPA's Attestation Standards and the ISAEs* provides answers to some of the more commonly asked questions about performing and reporting in SOC 2 examinations internationally.

SOC 2 examinations may also be performed by a CPA (or equivalent, such as a professional accountant in public practice) licensed in a jurisdiction outside the U.S., if permitted to do so by laws and regulations of a government or other body that has jurisdiction over the performance of accountancy. These engagements are usually performed in accordance with the International Standard on Assurance Engagements (ISAE) 3000 Revised, *Assurance Engagements other than Audits or Reviews of Historical Financial Information* or equivalent local country standards.

.05 CONSIDERING THE APPROPRIATE PERIOD OF TIME FOR A SOC 2 EXAMINATION

Inquiry—Does the SOC 2 guide establish a minimum period of time for a type 2 SOC 2 examination?

Reply—The SOC 2 guide does not prescribe a minimum period of time for a SOC 2 examination. The period of time to be addressed by a SOC 2 examination is a business decision made by service organization management after considering the informational needs of intended users.

When determining whether to accept a SOC 2 engagement, the service auditor considers the period of time to be addressed and whether sufficient appropriate evidence is likely to be available to support an opinion on operating effectiveness. Although the determination of the appropriateness of the period of time is a matter of professional judgment, paragraph 2.46 of the SOC 2 guide provides an example that may help a service auditor make that determination. In the example, service organization management wishes to engage the service auditor to perform a type 2 examination for a period of less than two months. The example indicates that, in this situation, the service auditor may conclude that it is unlikely that sufficient appropriate evidence could be obtained to support an opinion.

Inquiry—What factors may the service auditor consider when evaluating whether the period of time is appropriate for the SOC 2 examination?

Reply—When evaluating whether the period of time is appropriate, the service auditor may consider the frequency with which designed controls are to be performed and whether those controls are likely to operate within the period of time to be addressed by the examination. For example, some controls may operate only cyclically. An employee benefit administrator may use different applications and controls during an open enrollment period. If the period addressed by the SOC 2 examination does not include the operation of controls during the open enrollment period, the service auditor may be unable to obtain sufficient appropriate evidence of the operation of those controls to support the opinion on control effectiveness for the period of time addressed by the examination. In that situation, the service auditor may discuss the issue with management and determine whether a different period of time may be more appropriate.

Inquiry—In certain circumstances, some controls that would ordinarily have operated during the period of time addressed by the examination do not operate because the circumstances that warrant their operation do not exist. For example, controls over new user identification and authentication may not operate if no new users were added to the system during the period of time addressed by the examination. When management informs the service auditor of this situation, what are the service auditor's responsibilities?

Reply—In this situation, the service auditor should consider the guidance in paragraph 3.156 of the SOC 2 guide. In most cases, the service auditor would (*a*) perform procedures to corroborate management's statements; (*b*) describe in section 4 of the SOC 2 report those procedures and the results thereof; and (*c*) consider whether to add additional language to the service auditor's report as discussed in paragraph 4.86 of the SOC 2 guide.

.06 LACK OF A BOARD OF DIRECTORS

Inquiry—Trust services criterion CC1.2 discusses the need for a board of directors that is independent from service organization management and exercises oversight of the development and performance of internal control. If a smaller, less complex service organization does not have an independent board of directors, how would the service auditor's opinion on the suitability of design of controls be affected?

Reply—TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* defines a board of directors as follows:

> Individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

This definition recognizes that smaller, less complex businesses may find it costly and unnecessary to attract independent board members. These entities generally have different control environments, which may be as effective as those in larger, more complex organizations. In the context of a smaller, less complex service organization, an owner-manager may have far greater personal oversight over organizational structure operations; the ability to affect ethical values; and the ability to attract, retain, and hold accountable service organization personnel. In addition, an owner-manager is likely to actively participate in the operation of key controls (by exercising a high level of supervision and review) to provide adequate oversight of internal control and to mitigate risks arising from the lack of segregation of duties that often exists in such organizations. When that is the case, a service auditor may conclude that the lack of a board of directors at a smaller, less complex service organization is unlikely to affect the achievement of the service organization's service commitments and system requirements.

In some situations, however, an owner-manager may not have the knowledge or competence to perform the oversight role without placing excessive reliance on company service organization management. In this situation, the lack of independent oversight may result in a breakdown in internal controls and increase the risk of fraud. In such cases, the service auditor evaluates the effect of the design deficiency on the service organization's achievement of its service commitments and system requirements; based on that evaluation, the service auditor may decide to modify the opinion on suitability of design in the SOC 2 report.

.07 SOC 2 EXAMINATION THAT ADDRESSES ADDITIONAL SUBJECT MATTERS AND ADDITIONAL CRITERIA

Inquiry—Can a service auditor issue a SOC 2 report that also addresses additional subject matters and additional criteria?

Reply—Paragraphs 1.50–1.54 of the SOC 2 guide discuss potential considerations when a service organization engages a service auditor to examine and report on subject matters in addition to the description of the service organization's system in accordance with the description criteria and the suitability of design and operating effectiveness of controls based

on the applicable trust services criteria (for example, compliance with HIPAA security requirements). In such cases, the service auditor examines and reports on whether the additional subject matter is presented in accordance with the additional suitable criteria used to evaluate it.

The determination to perform a SOC 2 examination that includes additional subject matter and additional criteria is predicated on service organization management providing the service auditor with the following:

- An appropriate description of the subject matter
- A description of the criteria identified by service organization management used to measure and present the subject matter
- If the criteria are related to controls, a description of the controls intended to meet the control-related criteria
- An assertion by service organization management regarding the additional subject matter or criteria

In addition to the factors above, service organization management also needs to evaluate whether the principal service commitments and system requirements disclosed need to include service commitments or system requirements related to the additional subject matter and additional criteria.

The service auditor performs procedures to obtain sufficient appropriate evidence related to the additional subject matter and additional criteria and identifies in the service auditor's report the additional subject matter being reported on and the additional criteria being used to evaluate the subject matter. Paragraphs 1.53–1.54 of the SOC 2 guide discuss factors for the service auditor to consider when service organization management requests that the report include a description of the service auditor's tests of controls or procedures performed to evaluate the existing or additional subject matter against the existing or additional criteria and the detailed results of those tests.

When forming an opinion on the additional subject matter and the additional criteria used to evaluate the subject matter, the service auditor considers the effects of identified deficiencies on the additional subject matter evaluated using the trust services criteria, the subject matter evaluated using the additional criteria, or both. When considering the effects of those deficiencies on the service organization's ability to achieve one or more of the service commitments and system requirements, the service auditor exercises professional judgment, including the consideration of materiality as discussed in FAQ .11 and in the discussion paper *Materiality Considerations for Attestation Engagements Involving Aspects of Subject Matters That Cannot Be Quantitatively Measured*.

.08 USE OF SAMPLING

Inquiry—How does a service auditor use sampling in a SOC 2 examination?

Reply—When determining whether sampling is an appropriate strategy for testing controls in a SOC 2 examination, paragraph 3.142 of the SOC 2 guide indicates that the service auditor should consider the following:

a. The characteristics of the population of the controls to be tested, including the nature of the controls
b. Whether the population is made up of homogenous items

c. The frequency of the controls' application
d. The expected deviation rate

For example, if a control operates frequently, the service auditor may decide to use sampling when testing the operating effectiveness of the control. In this case, AICPA Audit Guide *Audit Sampling* may be useful to the service auditor.

Sampling, however, may not always be an appropriate strategy for testing controls in a SOC 2 examination. Paragraph 3.143 of the SOC 2 guide provides the following examples of situations in which sampling may not be appropriate:

a. Due to the design of one or more systems, it may not be possible to give every item in the population a chance of being selected for the sample.

b. The service auditor may determine that a 100 percent test of the control using data analytics is necessary because even a one-time failure of the control could result in a material deficiency in the operating effectiveness of controls.

c. The service auditor may conclude that it is more efficient and effective to perform a 100 percent test of the data evidencing the effective operation of the control than selecting and testing a sample.

When applying professional judgment regarding the use of audit sampling, the service auditor considers whether the assumptions for sample-based testing have been met.

Inquiry—When the service auditor has determined that sampling is the appropriate approach, what items would need to be documented in the working papers for a SOC 2 examination?

Reply—According to Paragraph 3.96 of AICPA Guide *Audit Sampling*, AU-C section 230, *Audit Documentation*, establishes requirements and provides guidance regarding the auditor's responsibility to document audit procedures. The guide also provides examples of items that auditors may document when using sampling, some of which may help service auditors decide what to document when using sampling in a SOC 2 examination. Based on that guidance, when using sampling, a service auditor may document, among others, the following items:[6]

- A description of the control being tested
- The definition of the population and the sampling unit, including how the service auditor considered the completeness of the population
- The definition of the deviation condition
- The method of sample size determination
- The method of sample selection
- The selected sample items
- A description of how the sampling procedure was performed
- The evaluation of the sample and the overall conclusion

[6] Paragraph 3.96 in the AICPA audit sampling guide states that, in some instances, sample size inputs such as acceptable risk of overreliance, tolerable rate of deviation, and expected deviation rate are built into firm-wide sample size tables. In these instances, reference to firm sample size guidance is sufficient (that is, each team does not need to document inputs that are implicit in the firm's sample size tables).

Paragraph .A14 of AU-C section 230 provides several examples of how an auditor can identify selected sample items in documentation. Documenting the basis for the sample size selected (for example, the parameters considered) can clarify how the sample size relates to the overall audit strategy.

.09 LAWS AND REGULATIONS

Inquiry—Does a service auditor's opinion in a SOC 2 examination address the service organization's compliance with relevant laws and regulations?

Reply—No. A SOC 2 examination addresses only the design and, in a type 2 examination, the operating effectiveness of controls that support the service organization's compliance with specified laws and regulations. For example, when a service organization is subject to relevant laws and regulations, service organization management would identify system requirements to support the service organization's ability to comply with such laws and regulations; the service auditor would test controls to achieve such system requirements during the SOC 2 examination, and the opinion would address the design and, in a type 2 examination, the effectiveness of such controls. The SOC 2 report does not provide an opinion on whether the service organization complied with relevant laws or regulations.

If service organization management wanted to obtain an opinion on compliance with relevant laws or regulations, it may engage a practitioner to examine and report on compliance with requirements of specified laws and regulations. Such an examination would be performed in accordance with AT-C section 315, *Compliance Attestation*.

.10 PROCEDURES FOR TESTING OPERATING EFFECTIVENESS

Inquiry—Can a service auditor obtain sufficient appropriate evidence about the operating effectiveness of controls in a SOC 2 examination through the performance of inquiry alone?

Reply—No, paragraph 3.116 of the SOC 2 guide clarifies that inquiry alone is unlikely to provide sufficient appropriate evidence of the operating effectiveness of controls. That paragraph also provides guidance on other types of procedures a service auditor may perform to obtain sufficient appropriate evidence of the operating effectiveness of controls. For example, the service auditor may also perform walk-throughs, observation, inspection of documents, and reperformance.

.11 CONSIDERATION OF MATERIALITY IN A SOC 2 EXAMINATION

Inquiry—How does a service auditor consider materiality in a SOC 2 examination?

Reply—The service auditor's consideration of materiality in a SOC 2 examination is discussed throughout the SOC 2 guide. Among other things, such guidance makes the following two key points:

- The consideration of materiality is a matter of professional judgment and is affected by the service auditor's perception of the common information needs of the broad range of report users as a group and on whether misstatements could

reasonably be expected to influence the relevant decisions made by the broad range of report users.
- The service auditor should reconsider materiality if the service auditor becomes aware of information during the engagement that would have caused the service auditor to have initially determined a different materiality.

The service auditor's considerations during various stages of the examination are discussed throughout the guide. Specifically:

- Chapter 2 of the guide discusses the responsibilities of the service auditor during engagement acceptance and planning and includes considering both qualitative and quantitative materiality factors when establishing an overall strategy.

- Chapter 3 discusses the service auditor's consideration of qualitative and quantitative factors when evaluating whether the description presents the system that was designed and implemented in accordance with the description criteria; when evaluating whether controls were suitably designed; and in a type 2 examination, when evaluating whether controls were operating effectively.

- Chapter 4 discusses materiality considerations when forming the opinion on the description, the suitability of design of controls, and in a type 2 examination, the operating effectiveness of controls.

As most service auditors already know, because aspects of the subject matters considered in a SOC 2 examination cannot be quantitatively measured, considering materiality when planning, performing, and reporting in these engagements can be very challenging.

To further assist practitioners with the challenges surrounding the consideration of materiality in engagements such as these, the AICPA established, through its Assurance Services Executive Committee (ASEC), the materiality Working Group (working group) to assess how practitioners consider materiality in examination and review attestation engagements involving aspects of subject matters that cannot be quantitatively measured. As a result of the working group's efforts, the staff published nonauthoritative guidance to assist practitioners with making professional judgments regarding materiality in such examination and review engagements. Service auditors may find such guidance — which can be found in the discussion paper *Materiality Considerations For Attestation Engagements Involving Aspects Of Subject Matters That Cannot Be Quantitatively Measured* — helpful when considering materiality in a SOC 2 examination.

.12 SOC 3® EXAMINATIONS

Inquiry—Can service organization management elect to use the carve-out method for a subservice organization for a SOC 3® report?

Reply—Yes, use of the carve-out method is permitted; however, service organization management considers whether use of the carve-out method for presenting a subservice organization in a SOC 3 report may be misleading to users. As discussed in paragraph 2.170 of the SOC 2 guide, a SOC 3 report contains a description of the boundaries of the system. That description, which is also referenced in management's assertion, is part of the SOC 3 report as illustrated in appendix F of the SOC 2 guide. In some cases, that description would

disclose the services performed by the carved-out subservice organization because that is likely to affect the boundary of the system to be addressed in the examination. In that case, it may provide users with the information they need to understand the role of the subservice organization and the activities the service organization performs to monitor the subservice organization.

If, however, the description of the boundaries of the system does not contain sufficient information for users to understand how the carved-out subservice organization may affect the achievement of the service organization's service commitments and system requirements in the SOC 3 report, there may be a risk that the report will be misleading to report users.

If the service auditor believes that there is a risk that the SOC 3 report will be misleading to report users, paragraph 4.117 of the SOC 2 guide indicates that the service auditor may consider whether to restrict the use of the SOC 3 report to an appropriate subset of potential report users, such as user entities that have access to the SOC 2 report or to a SOC 3 report from the subservice organization. (From a practical standpoint, the service auditor is likely to have discussed the need to restrict the use of a SOC 3 report with service organization management during engagement acceptance.)

Inquiry—Can a service auditor issue a type 1 SOC 3 report following completion of a type 1 SOC 2 report?

Reply—No. Appendix B of the SOC 2 guide, *Comparison of SOC 1®, SOC 2® and SOC 3® Examinations and Related Reports*, compares the components of each of the SOC reports. As that table indicates, there are type 1 and type 2 versions of both a SOC 1 and SOC 2 report, but there is no type 1 equivalent for a SOC 3 report.

The AICPA did not develop or include in the SOC 2 guide a type 1 SOC 3 report because of concerns that general users, who are the intended users of a SOC 3 report, might not understand that controls that have been suitably designed and implemented do not necessarily operate effectively. To prevent such misunderstanding, a SOC 3 report includes the following elements, as identified in paragraph 4.111 of the SOC 2 guide:

a. An assertion by service organization service organization management about whether the controls were effective throughout the period.
b. An opinion by the service auditor on service organization management's assertion about whether controls within the system were effective throughout the period.

.13 SOC LOGO FOR CPAS

Inquiry—How can a CPA firm use the SOC for Service Organizations Logo (SOC logo)?

Reply—A CPA firm may use the SOC logo in connection with marketing, promoting and performing the SOC 1, SOC 2, or SOC 3 examinations. To display or use the SOC logo, a CPA firm should comply with the terms, conditions, and guidelines for CPAs and the requirements of the Board of Accountancy in the state(s) or, for a jurisdiction outside the U.S., a government or other body that has jurisdiction over the performance of accountancy in which it practices.

The AICPA has recently revised those guidelines to broaden the ways in which CPA firms can use the SOC logo to promote their SOC practices. The new guidelines (available at www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-service-organizations-logo-guidelines-cpa.pdf) clarify that CPA firms may use or display the SOC logo to market and promote the activities outlined in paragraph 2 of the guidelines, provided the logo is hyperlinked to www.aicpa.org/soc4so. CPA firms may use and display the SOC logo in several ways, including the following:

- On their websites
- In brochures, report packages or engagement proposals
- In PowerPoint presentations
- In the firm's social media posts
- In printed physical media

The SOC logo is not to be used in an individual CPA's email signature block or in an individual CPA's social media posts.

The SOC for Service Organization logo may be used by service organizations that obtain certain SOC services. The revised guidelines (available at www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-logo-guidelines-service-organization.pdf) broaden the ways in which the logo may be used or displayed to market and promote the service organization's SOC 1, SOC 2, or SOC 3 reports.

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.