AU-C Section 9402

Audit Considerations Relating to an Entity Using a Service Organization: Auditing Interpretations of AU-C Section 402

1. Considerations Related to the Use of a SOC 2® [1] Report in an Audit of a User Entity's Financial Statements

.01 *Question* — AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization*,* defines a *user entity* as an entity that uses a service organization and whose financial statements are being audited. It also defines a *service organization* as an organization or segment of an organization that provides services to user entities that are relevant to those user entities' internal control over financial reporting (ICFR). When a service organization does not provide a SOC 1® [2] report or a similar report issued under, for example, International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, but does provide a SOC 2 report relevant to the services used by the user entity, may the auditor of a user entity's financial statements (a user auditor) use the SOC 2® report to meet the objectives of AU-C section 402?

.02 *Interpretation* — AU-C section 402 contains requirements and guidance for a user auditor on (*a*) obtaining an understanding of the nature and significance of the services provided by a service organization and their effect on the user entity's internal control relevant to the audit, sufficient to identify and assess the risks of material misstatement, and (*b*) designing and performing audit procedures responsive to those risks.[3]

---

[1] 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. A SOC 2® engagement is an examination of controls over the security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed by the system. It is performed under AT-C section 205, *Assertion-Based Examination Engagements.* The AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* is an interpretive publication that addresses SOC 2 engagements and provides recommendations on the application of AT-C section 205 to such engagements.

* All AU-C sections can be found in AICPA *Professional Standards.*

[2] A SOC 1 engagement is an examination engagement performed under AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.*

[3] This paragraph is replaced with the following to reflect the issuance of SAS No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, which has been codified in AU-C section 315:

> AU-C section 402 contains requirements and guidance for a user auditor on (*a*) obtaining an understanding of the nature and significance of the services provided by a service organization and their effect on the user entity's system of internal control, sufficient to provide an appropriate basis for the identification and assessment of the risks of material misstatement, and (*b*) designing and performing audit procedures responsive to those risks.

SAS No. 145, issued in October 2021, is effective for audits of financial statements for periods ending on or after December 15, 2023. The distinct presentation of this content (as gray shaded) is intended to aid the reader in differentiating content that may not be effective for the reader's purposes. This paragraph applies when SAS No. 145 is early implemented or upon its effective date.

.03 A service auditor performs a SOC 1 engagement under AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*,† which is an attestation standard specifically designed to enable a service auditor to report on management of a service organization's description of its system (description) and the service organization's controls included in the description that are relevant to a user entity's ICFR. A SOC 1 report addresses the risks related to a financial statement audit and is intended to complement AU-C section 402. As such, a SOC 1 report or an equivalent report issued under, for example, ISAE 3402, is the preferred report for use in an audit of a user entity's financial statements. When a SOC 1 report is unavailable, a user auditor may be able to obtain relevant information from other types of attestation reports. One such report is a report on an examination of controls at a service organization relevant to one or more of the trust services categories of criteria, which include security, availability, processing integrity, confidentiality, and privacy (SOC 2 report).

.04 Although a SOC 2 report may provide a user auditor with information about the nature of the services provided by the service organization and the suitability of the design and operating effectiveness of certain controls at the service organization, a SOC 2 report is not specifically designed to address controls at a service organization relevant to a user entity's ICFR and therefore is unlikely to achieve the intent of the requirements in AU-C section 402. Because a SOC 2 report is not designed to serve the same purpose as a SOC 1 report, an understanding of the differences between these two types of reports may assist a user auditor in evaluating the sufficiency and appropriateness of the evidence provided by a SOC 2 report in an audit of a user entity's financial statements. The following are some considerations when determining whether a SOC 2 report may be used in the audit of a user entity's financial statements and some of the limitations of using a SOC 2 report in these circumstances:

- *Purpose of the report*. A SOC 2 engagement, which is performed under AT-C section 205, *Assertion-Based Examination Engagements*, addresses controls at a service organization that are intended to provide reasonable assurance that the service organization's service commitments and system requirements are achieved, based on the applicable trust services criteria. Importantly, a SOC 2 engagement is not designed to address the services performed by a service organization that are likely to be relevant to a user entity's ICFR and therefore is unlikely to completely address the effect that the service organization has on a user entity's financial reporting.

- *Potential overlap with financial reporting.* A SOC 2 report may address certain areas that could be relevant to a user entity's ICFR, such as logical access and change management. However, in a SOC 2 engagement, the service auditor's tests of such controls may be designed to address a different set of risks and are unlikely to provide sufficient appropriate audit evidence regarding controls at a service organization relevant to a user entity's ICFR. For example, although the change management criterion in a SOC 2 engagement[4] addresses attributes in the change management life cycle that may be relevant to a user entity's ICFR (for example, testing, approval, and implementation of changes into production), the service organization's service commitments and system requirements in a SOC 2 engagement typically address the effect that the change has on the security and availability of systems and therefore may not address the completeness, accuracy, and timeliness of the processing and reporting of transactions and balances relevant to a user entity's ICFR.

- *Scope of the report and understanding of the nature of the services provided by the service organization.* Because a SOC 2 report is not specifically designed to address services relevant to a user entity's ICFR, the description in a SOC 2 report may not include all the services, reports, statements, processes, and controls relevant to a user entity's ICFR. In contrast, the criteria for

† All AT-C sections can be found in AICPA *Professional Standards.*

[4] See CC8.1 in the *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

the description in AT-C section 320 require that such information be included in the description in a SOC 1 report.[5] Accordingly, the use of a SOC 2 report in an audit of a user entity's financial statements involves careful evaluation of the scope of the report and the content of the description in determining the relevance of the report to a user entity's ICFR.

- *Complementary user entity controls.* In a SOC 2 report, complementary user entity controls (CUECs) represent controls that management of the service organization assumed, in the design of the service organization's system, would be implemented by user entities and are necessary, in combination with controls at the service organization to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, based on the applicable trust services criteria. However, in a SOC 1 report, the CUECs represent controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by user entities and are necessary to achieve a set of control objectives stated in the description that are relevant to user entities' ICFR. As a result, it is unlikely that a SOC 2 report will include the same set of CUECs that would be included in a SOC 1 report addressing similar services. The user auditor's careful analysis of the SOC 2 report is needed to identify (*a*) the CUECs included in a SOC 2 report, if any, that would need to be implemented at a user entity to achieve control objectives relevant to the user entity's ICFR, and (*b*) other controls that would need to be implemented by a user entity to mitigate the risks to the user entity's ICFR resulting from the use of a service organization (these controls are not identified as CUECs in a SOC 2 report). For example, if a service organization is responsible for performing logical access administration for users at the user entity, a SOC 1 report may include a CUEC indicating that the user entity provides complete, accurate, and appropriately authorized instructions for access changes. However, in a SOC 2 report, this control may not be identified as a CUEC because the service organization is able to meet its service commitments to administer access based on the instructions provided by the user entity, regardless of the completeness and accuracy of those instructions.

  To identify additional user responsibilities relevant to a user entity's ICFR that are not presented in a SOC 2 report as CUECs, a user auditor may review the following:

  - Contracts, service level agreements, or other documents between the user entity and the service organization to obtain an understanding of the services performed
  - The extent to which those services are, or are not, addressed by the SOC 2 report
  - The service organization's and user entity's responsibilities, even if not identified in the SOC 2 report as SOC 2–related CUECs

- *Access to the SOC 2 report not provided to downstream users.* For carved-out subservice organizations, paragraph .A70 of AT-C section 320 indicates that a user entity is also considered a user entity of the service organization's subservice organizations if controls at the subservice organizations are relevant to the user entity's ICFR. Paragraph .A70 refers to such user entities as *indirect* or *downstream* user entities. Because the definition of *user entity* in a SOC 2 engagement is substantially the same as it is in a SOC 1 engagement, downstream user entities of a SOC 2 report would be considered intended users of a SOC 2 report.

- *Services provided by subservice organizations likely to be relevant to a user entity's ICFR.* An additional user auditor consideration is that the scope of a SOC 2 report may not include all the services provided by subservice organizations that are likely to be relevant to a user entity's ICFR. For example, although a service provider that provides pricing data for investments may be a relevant subservice organization for a SOC 1 report, it may not be relevant to the SOC 2 report based on the applicable trust services criteria, which are intended to address the service organization's service commitments and system requirements.

[5] Paragraph .15 of AT-C section 320.

- *Information prepared for user entities.* The information included in a SOC 2 report may address information prepared for user entities that is relevant to the service organization's service commitments — for example, system uptime reports to address availability commitments and user access listings related to security commitments — but may not address other types of information and reports that would be relevant to a user entity's ICFR. In evaluating the usefulness of a SOC 2 report in an audit of a user entity's financial statements, relevant considerations may include whether the scope of the SOC 2 report includes controls over the completeness and accuracy of the reports provided to user entities that are relevant to the user entities' ICFR. For example, a SOC 2 report that addresses an investment management system may include security reports such as user access lists or system availability reports for the application but may not include reports relevant to a user entity's financial transactions such as investment positions or transactions.

- *Intended users of the report.* The restricted-use paragraph in a type 2 SOC 2 report indicates that the intended users of a SOC 2 report include user entities of the system during some or all of the period covered by the report and practitioners providing services to such user entities. A user auditor would qualify as a practitioner providing services to a user entity and therefore would be considered an intended user of a SOC 2 report.

- *Service auditor's consideration of deficiencies.* In a SOC 2 engagement, the service auditor evaluates identified deficiencies in the design or operating effectiveness of controls based on their effect on the service organization's service commitments and system requirements, as opposed to their effect on the service organization's identified control objectives, as is the case in a SOC 1 engagement.

.05 The following table summarizes how a SOC 2 report may address the requirements in paragraph .09 of AU-C section 402:

Requirement in Paragraph .09 of AU-C Section 402	How a SOC 2 Report May Address the Requirement in Paragraph .09 of AU-C Section 402
09. A user auditor should obtain an understanding of how the user entity uses the services of a service organization in the user entity's operations, including the following:	
a. The nature of the services provided by the service organization and the significance of those services to the user entity, including their effect on the user entity's internal control	A SOC 2 report may be useful in understanding the nature of some of the services provided by the service organization, including the service organization's service commitments and controls relative to categories of trust services criteria such as security and processing integrity. However, due to the intended scope of the report, it may not address all the services relevant to a user entity's internal control over financial reporting.
b. The nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization	A SOC 2 report is unlikely to address the nature and materiality of transactions processed by the service organization unless it includes the processing integrity category of the trust services criteria.

c. The degree of interaction between the activities of the service organization and those of the user entity	A SOC 2 report may address the interaction between the activities of the service organization and those of the user entity especially as it relates to the service commitments that the service organization has made to its user entities based on the scope of the report.
d. The nature of the relationship between the user entity and the service organization, including the relevant contractual terms for the activities undertaken by the service organization	Like a SOC 1 report, a SOC 2 report is unlikely to address the relevant contractual terms; however, it will provide some information about the relationship between the user entity and the service organization. For example, the disclosure of the service organization's key service commitments relative to the trust services categories of criteria that are addressed by the SOC 2 report may assist the user auditor in understanding the nature of the relationship between the user entity and the service organization.

[Issue Date: December 2022.]