August 2019

AICPA

Common deficiencies peer reviewers noted in SOC 1® and SOC 2® examinations

Contents

Promoting quality and effectiveness of practices through peer review

To be admitted to or retain their AICPA membership, members in the public accounting practice in the United States or its territories must practice as partners or employees of firms enrolled in an approved practice-monitoring program. If practicing in firms that are not eligible to enroll, members must enroll in an approved practice-monitoring program if the services such a firm or individual perform are within the scope of the AICPA's practice-monitoring standards and the firm or individual issues reports purporting to be in accordance with AICPA professional standards.

Firms have peer reviews because of the public interest in the quality of the accounting, auditing and attestation services public accounting firms provide. In addition, firms indicate that peer review contributes to the quality and effectiveness of their practices. Furthermore, most state boards of accountancy require their licensees to undergo peer review, or compliance assurance, to practice in their states. Other regulators require peer review to perform engagements and issue reports under their standards.

Firms are required to perform engagements in accordance with professional standards and, accordingly, the standards are the basis for peer reviews. You can find training and frequently asked questions about the AICPA Peer Review Program here.

This document presents the most common deficiencies noted in peer reviews of SOC 1 and SOC 2 examinations[1] for periods ending between June 30, 2016, and March 31, 2018.[2] The requirements and guidance for performing and reporting on these engagements are in the following sources:

- *SOC 1 — SOC for Service Organizations: ICFR*. AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*,[3] and AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®)* (SOC 1 guide)
- *SOC 2 — SOC for Service Organizations: Trust Services Criteria.* AT-C section 205, *Examination Engagements*, and 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)

Failure to obtain the appropriate competence required under the attestation standards to properly perform a SOC engagement

Paragraph .32 of AT-C section 105, *Concepts Common to All Attestation Engagements*, states the engagement partner should be satisfied that the engagement team, and any practitioner's external specialists, collectively, have the appropriate competence, including knowledge of the subject matter, and capabilities to:

a. perform the engagement in accordance with professional standards and applicable legal and regulatory requirements and
b. enable the issuance of a practitioner's report that is appropriate in the circumstances.

Peer reviewers noted instances in which engagement personnel were not familiar with the applicable professional standards related to reporting on controls at service organizations or failed to perform the engagement in accordance with the most recent applicable professional standards. In other instances, peer reviewers noted a lack of understanding of the type of engagement that should have been performed and the controls that the SOC report should have addressed. For instance, a SOC 1 engagement that should have addressed controls at the service organization relevant to user entities' internal control over financial reporting was instead performed on controls at the service organization relevant to the service organization's financial statements.

To perform high-quality SOC engagements, engagement team members need to possess the appropriate competence and skills to perform these highly specialized engagements. Such competencies might include, but are not limited to, an understanding of the service organization's industry and business, systems used to provide services, and business and IT processes and controls, as well as experience evaluating the suitability of design and operating effectiveness of relevant controls. Additional guidance related to this topic is contained in the application guidance in paragraphs .A59–.A60 of AT-C section 105 and paragraphs 2.39–2.42 of the SOC 2 guide.

[1] 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.

[2] Because of the timing of when peer reviews are performed, there is a lag between the period end of the engagement and when a matter is included in reports on peer review findings (MFC reports). Peer reviews are due six months after a firm's peer review year end. A firm's peer review would cover engagements with period ends during the peer review year (or the "as of" date for type 1 reports). As an example, if a firm's peer review year is Jan. 1, 2014, to Dec. 31, 2014, its peer review is not due until June 30, 2015. Therefore, a Jan. 31, 2014, period-end engagement would not be included in the MFC report until about June 30, 2015. However, a Dec. 31, 2014, period-end engagement in the same scenario would also be included in the MFC report around June 30, 2015. Refer to aicpa.org/prsummary for more information about peer review.

[3] All AT-C sections are in AICPA *Professional Standards*.

Failure to prepare reports in accordance with professional standards

The elements required to be included in a service auditor's examination report for a SOC 1 engagement are described in paragraphs .40–.41 of AT-C section 320 and paragraph 5.18 of the SOC 1 guide. For a SOC 2 engagement, the required elements are described in paragraphs .63–.65 of AT-C section 205 and paragraph 4.32 of the SOC 2 guide. Peer reviewers noted the following issues relevant to service auditor's reports:

- Failure to date the service auditor's report
- Failure to appropriately identify the criteria used for evaluation
- Failure to include appropriate language related to subservice organizations, complementary subservice organization controls, and complementary user entity controls
- Failure to identify other information not covered by the service auditor's report that is included in a document containing the service auditor's report (Paragraph 5.24 of the SOC 1 guide and paragraph 4.96 of the SOC 2 guide provide additional clarification of requirements related to other information not covered by the service auditor's report.)
- In a SOC 1 engagement, incorrectly including in management's assertion the standard verbiage for an assertion for a SOC 2 engagement

Failure to describe the service auditor's tests of controls and results of tests in accordance with professional standards

Requirements related to describing tests of controls and results of tests are included in paragraph .40k of AT-C section 320, paragraph 5.18 of the SOC 1 guide, and paragraphs 4.15–4.22 of the SOC 2 guide. Peer reviewers noted the following types of issues, among others, with respect to the service auditor's description of tests of controls and the results of tests:

- Deviations noted in the working papers were not included in the service auditor's description of tests of controls and results of tests.
- Deviations identified in the description of tests of controls and results did not include the size of the sample and the number of deviations.
- In SOC 2 engagements in which the operating effectiveness of controls could not be tested because the controls did not operate during the period covered by the service auditor's report, the description of tests of controls and results incorrectly indicated that the controls were tested with no exceptions noted (paragraph 4.86 of the SOC 2 guide provides additional clarification on this topic).

Failure to adequately document the nature, timing and extent of procedures performed

The documentation requirements for all examination attestation engagements, including SOC 1 and SOC 2 engagements, are included in paragraphs .34–.41 of AT-C section 105 and paragraphs .87–.89 of AT-C section 205. Paragraph .87 of AT-C section 205 states that the service auditor should prepare engagement documentation that is sufficient to determine the following:

1. The nature, timing and extent of procedures performed to comply with relevant AT-C sections and applicable legal and regulatory requirements, including the identifying characteristics of the specific items or matters tested, who performed the work and the date the work was completed, and who reviewed the work performed and the date and extent of such review
2. The results of the procedures performed and evidence obtained

The application material contained in paragraph .A119 of AT-C section 205 further explains that in applying professional judgment to assess the extent of documentation to be prepared and retained, the service auditor may consider what is necessary to provide an experienced practitioner, having no previous connection with the engagement, with an understanding of the work performed and the basis of the principal decisions made.

Examples of issues noted with respect to this topic include:

- Based on the documentation, insufficient evidence to support the opinion regarding
  - — the presentation of the description of the service organization's system
  - — the operating effectiveness of controls, including, for example,
    - working papers related to tests of controls show the results of tests but not the nature, timing, and extent of the procedures performed
    - testing of controls for only a portion of the period covered by the report or after the period covered by the report
    - testing the operating effectiveness of controls through inquiry alone
- Failure to identify who performed the work and when the work was completed

Failure to adequately document sampling methodology

Paragraph .31 of AT-C section 205 provides guidance about how to perform sampling during an attestation engagement. However, if the sampling methodology is not documented, then the reviewer may not be able to evaluate whether the procedure provided appropriate evidence. Paragraph .A28 of AT-C section 205 indicates that the AICPA Audit Guide *Audit Sampling* provides guidance that may be useful to a service auditor using sampling in performing attestation procedures.

Additional guidance related to sampling is discussed in paragraphs 4.111–4.112 of the SOC 1 guide and paragraphs 3.142–3.146 of the SOC 2 guide.

Peer reviewers noted the following issues:

- No documentation about whether the sample sizes were appropriate and items selected were representative of the population
- No documentation of the service auditor's consideration of the impact of identified deviations on conclusions reached about the operating effectiveness of controls
- No documentation of specific items tested
- Number of sample items actually tested did not correspond to the number of sample items that should have been tested as documented in the sampling methodology working papers

Failure to adequately document materiality considerations

Paragraph .16 of AT-C section 205 states the service auditor should consider materiality for the subject matter of the engagement when establishing the overall engagement strategy. Paragraph .19 of AT-C section 320 indicates that, in a SOC 1 engagement, the service auditor's consideration of materiality should include the fair presentation of management's description of the service organization's system, the suitability of the design of controls to achieve the related control objectives stated in the description, and in the case of a type 2 report, the operating effectiveness of the controls to achieve the related control objectives stated in the description.

Similarly, in a SOC 2 engagement, the service auditor's consideration of materiality includes the presentation of management's description of the service organization's system in accordance with the description criteria, the suitability of the design of controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and in the case of a type 2 report, the operating effectiveness of controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The application guidance contained in paragraphs .A15–.A21 of AT-C section 205 provides further information about the importance of materiality considerations related to qualitative factors in addition to any quantitative factors, as well as professional judgments about materiality based on the information needs of users.

Additional guidance related to materiality is provided in paragraphs 4.17–4.19, 4.60, 4.79, 4.171, and 5.03 of the SOC 1 guide and paragraphs 2.104–2.109, 3.05–3.08, 3.72–3.78, 3.161–3.165, 4.16, and 4.54–4.55 of the SOC 2 guide.

Peer reviewers noted inadequate documentation of how materiality was considered with respect to:

- The presentation of the system description
- The suitability of the design of controls
- The operating effectiveness of controls

Failure to adequately document procedures relating to risk assessment and the linkage of risks to the procedures performed

Paragraphs .18–.20 of AT-C section 205 address the service auditor's responsibilities related to performing risk assessments and responding to the risks of material misstatement identified and assessed by the service auditor (see also paragraphs .20–.23 of AT-C section 320 for SOC 1 engagements). Paragraphs .21–.31 of AT-C section 205 provide guidance regarding the linkage of identified risks to the nature, timing, and extent of procedures to be performed (see also paragraph .24 of AT-C section 320 for SOC 1 engagements). Additional guidance related to responding to assessed risk and obtaining evidence is provided beginning at paragraph 4.01 of the SOC 1 guide and paragraph 3.01 of the SOC 2 guide.

Peer reviewers noted the following issues:

- For SOC 1 engagements, working papers did not identify the risks that threaten the achievement of the control objectives and, for SOC 2 engagements, did not identify the risks that threaten the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria.
- Working papers did not adequately document risk assessment procedures performed, such as review of management's description, inquiry of management, and walk-through of applicable controls.

Failure to adequately document the service auditor's conclusions about whether the subject matter of the engagement is appropriate and the criteria used for preparation and evaluation are suitable

Paragraph .25 of AT-C section 105 states the service auditor should determine whether the subject matter is appropriate and the criteria to be applied in the preparation and evaluation of the subject matter are suitable and will be available to intended users. Additional guidance related to assessing the suitability of the criteria used for the preparation and evaluation of the subject matter and the appropriateness of the subject matter is provided in paragraphs 3.95–3.96 of the SOC 1 guide and paragraphs 2.44–2.65 of the SOC 2 guide.

Peer reviewers noted insufficient documentation of the service auditor's consideration of the following:

- The suitability of the criteria
- For a SOC 1 engagement, whether the control objectives were reasonable in the circumstances if no information technology general controls were identified

> Paragraph .25 of AT-C section 105 states the service auditor should determine whether the subject matter is appropriate and the criteria to be applied in the preparation and evaluation of the subject matter are suitable and will be available to intended users.

Failure to adequately document nonattest services the firm performed when determining the effect on the service auditor's independence

Paragraph .24 of AT-C section 105 discusses independence requirements for service auditors performing attestation engagements. The "Independence Rule" (ET section 1.200.001)[4] of the AICPA Code of Professional Conduct establishes independence requirements for attestation engagements. The "Independence Standards for Engagements Performed in Accordance With Statements on Standards for Attestation Engagements" subtopic (ET section 1.297) of the "Independence Rule" establishes special independence requirements for a service auditor who provides services under the attestation standards. The "Nonattest Services" subtopic (ET section 1.295) addresses documentation requirements related to nonattest services performed for attest clients.

Peer reviewers noted the following issues:

- Inadequate documentation of management and service auditor responsibilities related to nonattest services, including
  - the management-level individuals responsible for overseeing, reviewing, and accepting such services
  - the skills, knowledge, and experience of the management-level individuals
- Failure to document the determination that performing the nonattest service would not impair independence

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

Failure to properly document the agreed-upon terms of the engagement with the engaging party

Paragraphs .07–.09 of AT-C section 205 address the requirements related to agreed-upon terms of the engagement that should be specified in an engagement letter or other suitable form of written agreement. Additional guidance related to engagement letters is provided in paragraphs 3.91–3.95 of the SOC 1 guide and paragraphs 2.70–2.78 of the SOC 2 guide.

On a SOC 2 engagement, the peer reviewer noted a new engagement letter was not obtained or amendments made to the original engagement letter to reflect the following changes in scope:

- Performing the engagement using the *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (TSP section 100)[5] instead of *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (TSP section 100A)
- Management's decision not to include the privacy criteria

Failure to obtain written representation letters and improper dating of representation letters

Paragraphs .50–.54 of AT-C section 205 address the service auditor's responsibility to obtain written representations from the responsible party (that is, management). Additional guidance related to representation letters is provided in paragraphs .36–.37 of AT-C section 320, paragraphs 4.178–4.191 of the SOC 1 guide, and paragraphs 3.197–3.212 of the SOC 2 guide. Illustrative examples of representation letters are included in appendixes B and C of the SOC 1 guide and appendix G of the SOC 2 guide.

Peer reviewers noted the following issues:

- Written representations not dated the same date as the service auditor's report
- Failure to obtain a management representation letter

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

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