



**AICPA<sup>®</sup>**

Peer Review  
Program

**QUESTIONS AND ANSWERS ABOUT  
THE AICPA PEER REVIEW PROGRAM**

**FIRMS THAT PERFORM EXAMINATIONS  
OF SERVICE ORGANIZATIONS**

**January 2023**

## Table of Contents

FIRMS THAT PERFORM EXAMINATIONS OF SERVICE ORGANIZATIONS.....	1
What are the characteristics of SOC for Service Organizations engagements?.....	1
I'm having difficulty finding a review team member with appropriate SOC experience. What are my options?.....	2
APPENDIX A.....	4
Reviewer Qualifications .....	4
Team Captain or Review Captain.....	4
Other Peer Reviewer or Reviewing Firm Qualification Considerations.....	5

## **FIRMS THAT PERFORM EXAMINATIONS OF SERVICE ORGANIZATIONS**

### **What are the characteristics of SOC for Service Organizations engagements?**

SOC for Service Organizations engagements include:

- SOC 1® - SOC for Service Organizations: ICFR (performed in accordance with AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* and the AICPA Guide *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (SOC 1®))
- SOC 2® - SOC for Service Organizations: Trust Services Criteria (performed under AT-C section 205, and the AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*)
- SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report (performed under AT-C section 205 and the AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*)

#### *SOC 1 Engagements*

The purpose of the report in a SOC 1 engagement is to provide management of the service organization, user entities and the independent auditors of user entities' financial statements with information and a service auditor's opinion about controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. The report enables the user auditor to perform risk assessment procedures and, if the report is a type 2 report, to use the report as audit evidence that controls at the service organization are operating effectively. A SOC 1 report is a restricted-use report, intended for use by user entities of the service organization and their financial statement auditors. SOC 1 engagements should not be used for reporting on controls over subject matter other than financial reporting. SOC 1 engagements are required to be examinations, are subject to a System Review and are must-select engagements.

#### *SOC 2 Engagements*

The purpose of the report in a SOC 2 engagement is to provide service organization management, user entities, business partners and other specified parties with information and a service auditor's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality or privacy. Many entities outsource tasks or functions that are unrelated to financial reporting to service organizations. SOC 2 reports are intended to meet the needs of a broad range of users that want to understand internal control at a service organization as it relates to the security, availability or processing integrity of the service organization's system, or the confidentiality or privacy of the data processed by that system. These reports may be

restricted in use but are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its controls. Similar to SOC 1 engagements, SOC 2 engagements provide for both Type 1 and Type 2 reports. Unlike SOC 1 engagements, the primary users of SOC 2 reports generally are not user auditors but rather management of the user entities that use the reports to make operational decisions. SOC 2 engagements are required to be examinations, are subject to a System Review and can be a must-select engagement.

### *SOC 3 Engagements*

The purpose of the report in a SOC 3 engagement is to provide interested parties with a service auditor's opinion about the effectiveness of controls at the service organization relevant to security, availability, processing integrity, confidentiality or privacy. Because of the different reporting requirements, a SOC 2 report is appropriate only for specified parties with sufficient knowledge and understanding of the service organization and the system, whereas a SOC 3 report is ordinarily appropriate for general use. The subject matter in a SOC 3 engagement is essentially the same as it is in a SOC 2 engagement, and the criteria for evaluating controls is the same as it is in a SOC 2 engagement. However, SOC 3 reports are designed to meet the needs of users who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality or privacy but do not need the detail included in a SOC 2 report. SOC 3 reports do not contain a detailed description of the service auditor's tests of the operating effectiveness of controls and the results of those tests. Instead, SOC 3 reports are general-use reports, which mean they may be used by anyone and therefore can be used by the service organization to market its services to potential customers.

[Back to top](#)

### **I'm having difficulty finding a review team member with appropriate SOC experience. What are my options?**

Consistent with other must-select engagements, if a firm performs SOC 1 or SOC 2 engagements, someone on the review team should have experience with these types of engagements. Peer reviews of firms that perform SOC 1 engagements will require a team member with SOC 1 experience; similarly, peer reviews of firms that perform SOC 2 engagements will require a team member with SOC 2 experience. Due to the specialized nature of SOC engagements, the PRB has determined that a specialist may be able to assist the team captain in lieu of a team member with SOC experience. The specialist should meet the criteria established by the AICPA in order to be approved to assist the review team in reviewing SOC 1 or SOC 2 engagements. Refer to [Appendix A](#) for the SOC specialist criteria.

Firms can use the reviewer search at [peerreview.aicpa.org/reviewer\\_search.html](https://peerreview.aicpa.org/reviewer_search.html) to identify a reviewer that meets the qualifications to review these engagements.

When a specialist is used, the team captain, as always, is responsible for supervising and conducting the review, communicating the review team's findings to the reviewed firm and

AE, preparing the report on the review and ensuring that peer review documentation is complete and submitted to the AE on a timely basis. The team captain should supervise and review the work performed by the specialist. The team captain will furnish instructions to the specialist regarding the manner in which materials and other notes relating to the review are to be accumulated to facilitate summarization of the review team's findings and conclusions. The specialist may be required to be available or participate in the exit conference.

[Back to top](#)

## APPENDIX A

### Reviewer Qualifications

Performing and reporting on a peer review requires the exercise of professional judgment by peers (see paragraphs .05 - .08 of Section 200 of the *Standards* for a discussion of a reviewer's responsibilities when performing a peer review). Accordingly, an individual serving as a reviewer on a System or Engagement Review should at a minimum:

- a. Be a member of the AICPA in good standing, licensed to practice as a CPA, and employed by or an owner of a firm enrolled in the program (that is, AICPA membership in active, non-suspended status).
- b. Be in public practice as a partner, manager, or person with equivalent responsibilities in the accounting or auditing practice or carrying out a quality control function in the CPA's firm. (Ref: par. .A3)
- c. Have current practice experience by performing or supervising accounting or auditing engagements in the CPA's firm or carrying out a quality control function in the firm, with reports dated within the last 18 months. (Ref: par. .A4)
- d. Have spent the last five years in the practice of public accounting in the accounting or auditing function.
- e. Be employed by or be the owner of a firm that has received a report with a peer review rating of pass or pass with scope limitations for its most recent peer review. (The report should have been accepted timely.) (Ref: par. .A5–.A6)
- f. Possess current knowledge of professional standards and experience related to the kind of practice and the industries of the engagements to be reviewed. (Ref: par. .A7)
- g. Obtain at least 48 hours of AICPA-required continuing professional education (CPE) every 3 years in subjects relating to accounting, auditing, and quality control with a minimum of 8 hours in any 1 year.
- h. Be free of restrictions from regulatory or governmental bodies on the CPA's ability to practice public accounting. (Ref: par. .A8)

[Back to top](#)

### Team Captain or Review Captain

In addition to adhering to the requirements in Section 200 to be a peer reviewer, a System Review team captain must be a partner. For an Engagement Review, the review captain is not required to be a partner. The team captain, or the review captain in limited circumstances, is required to ensure that all team members possess the necessary capabilities and competencies to perform assigned responsibilities and that team members are adequately supervised. The team captain or review captain has the ultimate responsibility for the review, including the work performed by team members.

Also, team captains and review captains should have completed peer review training that meets the requirements established by the PRB.

Additionally, to initially qualify as a team captain on a System Review or as a review captain on an Engagement Review, you must:

1. Complete the online peer reviewer curriculum [Becoming an AICPA Peer Review Team or Review Captain](#). The online peer reviewer curriculum is a series of modules that are similar to self-study on-demand courses. The modules must be taken sequentially, and each module contains a final exam that is designed to comply with NASBA CPE Standards and is similar to competency assessments in other on-demand self-study CPE courses.
2. Complete the [Becoming an AICPA Peer Review Team or Review Captain: Case Study Applications](#) in a live seminar format. This course features realistic case studies that encompass the most important elements of a system review, as well as several case studies pertaining to an engagement review.

The [Becoming an AICPA Peer Review Team or Review Captain: Case Study Applications](#) must be completed within the 12 months after the completion of the peer reviewer curriculum.

The following outlines the ongoing training requirements:

To maintain the qualifications of a team captain or of a review captain, you should participate in one of the following peer review training options within 12 months prior to the commencement of a review. Peer review training options include:

1. Attending the general session of the annual Peer Review Conference.
2. Completing the AICPA Peer Review Update on-demand self-study course. This course is an advanced reviewer training course that will be updated annually and cover recent changes to peer review guidance in addition to how recent changes in auditing or accounting standards impact peer review. This course will contain a final exam that is designed to meet the NASBA CPE Standards.
3. Attend an alternative course or conference session that has been approved by the PRB. For purposes of the ongoing training requirement, these alternative courses and conference session will be selected by the PRB. The PRB will not consider courses submitted by reviewers seeking consideration for an alternative course of their choosing.

[Back to top](#)

## **Other Peer Reviewer or Reviewing Firm Qualification Considerations**

Communications from regulatory, monitoring or enforcement bodies relating to allegations or investigations of a peer reviewer or reviewing firm's accounting and auditing practice, and notifications of limitations or restrictions on a peer reviewer or reviewing firm to practice, may impact the peer reviewer or reviewing firm's ability to perform the peer review. The peer reviewer or reviewing firm has a responsibility to inform the AE of such communications or notifications.

If required by the nature of the reviewed firm's practice, individuals with expertise in specialized areas may assist the review team in a consulting capacity. For example, IT specialists, statistical sampling specialists, actuaries, or experts in continuing professional education (CPE) may participate in certain segments of the review.

Some review teams may also need to engage a SOC specialist to assist the review team with reviewing SOC 1 or SOC 2 engagements. SOC specialists must meet specific criteria and have prior approval before an AE can approve them as part of a review team.

To become an approved specialist, the specialist candidate should complete a peer reviewer resume and indicate that they would like to serve as a specialist.

An individual serving as a SOC specialist on a System Review should at a minimum:

- a. Be currently active in public practice at a supervisory level for managing SOC 1 and/or SOC 2 examinations. To be considered currently active, a specialist should be presently involved in the SOC practice of a firm supervising one or more of the firm's SOC engagements.
- b. Be associated with a firm (or all firms if associated with more than one firm) that has received a report with a peer review rating of *pass*<sup>1</sup> for its most recent System Review that was accepted timely, ordinarily within the last three years and six months.
- c. Not be associated with an engagement that was deemed not performed or reported on in accordance with professional standards in all material respects on the specialist's firm's most recently accepted peer review.
- d. Possess current knowledge of professional standards applicable to SOC 1 and/or SOC 2 examinations, including Type 1 and Type 2 reports, qualified and unqualified reports, carve in/carve out engagements and engagements with and without relevant user entity controls.
- e. Have at least five years of recent experience in the practice of public accounting with a minimum of 500 hours of SSAE 16/SOC 1 and/or SysTrust/SOC 2 examinations.
- f. Have provided the AE with information that accurately reflects the qualifications of the specialist, which is updated on a timely basis.

---

<sup>1</sup> A peer review report with a rating of *pass* was previously referred to as an unmodified report (with or without a letter of comments). If a firm's most recent peer review rating was a *pass with deficiencies* or *fail*, the firm's members are not eligible to perform peer reviews.

[Back to top](#)