EXPOSURE DRAFT

PROPOSED CHANGES TO THE AICPA STANDARDS FOR PERFORMING AND REPORTING ON PEER REVIEWS

Scope of System Review and Must Select Engagements

June 1, 2012

Comments are requested by August 31, 2012

Prepared by the AICPA Peer Review Board for comment from persons interested in the AICPA Peer Review Program

Comments should be received by August 31, 2012 and addressed to
Rachelle Drummond, Technical Manager
AICPA Peer Review Program
American Institute of Certified Public Accountants
220 Leigh Farm Road, Durham, NC 27707-8110
or PR_expdraft@aicpa.org

CONTENTS

AICPA Peer Review Program

American Institute of CPAs
220 Leigh Farm Road
Durham, NC 27707-8110

June 1, 2012

The AICPA Peer Review Board (Board) approved issuance of this exposure draft, which contains proposals for review and comment by the AICPA's membership and other interested parties regarding revisions to the AICPA *Standards for Performing and Reporting on Peer Reviews ("Standards").*

Written comments or suggestions on any aspect of this exposure draft will be appreciated. To facilitate the Board's consideration, comments or suggestions should refer to the specific paragraphs and include supporting reasons for each comment or suggestion. Please limit your comments to those items presented in the exposure draft. Comments and responses should be sent to Rachelle Drummond, Technical Manager, AICPA Peer Review Program, AICPA, 220 Leigh Farm Road, Durham, NC 27707-8110 and must be received by August 31, 2012. Electronic submissions of comments or suggestions should be sent to PR_expdraft@aicpa.org by August 31, 2012.

Written comments on the exposure draft will become part of the public record of the AICPA Peer Review Program, and will be available on the AICPA website after October 19, 2012 for a period of one year.

The exposure draft includes an explanatory memorandum of the proposed revisions to the current *Standards* and Interpretations, explanations, background and other pertinent information, as well as marked excerpts from the current *Standards* and Interpretations to allow the reader to see all changes (i.e. items that are being deleted from the *Standards* and Interpretations are struck through, and new items are underlined). The Board is not required to expose changes to the Peer Review *Standards* Interpretations, but elected to do so to assist respondents with understanding the underlying intent of the proposed revisions to the *Standards*.

A copy of this exposure draft and the current *Standards* (effective for peer reviews commencing on or after January 1, 2009) are also available on the AICPA Peer Review website at http://www.aicpa.org/InterestAreas/PeerReview/Pages/PeerReviewHome.aspx.

Sincerely,

Theresa C. Golden

Tracey C. Golden
Chair
AICPA Peer Review Board

AICPA Peer Review Board
2011 – 2012

Tracey C. Golden, Chair*
James T. Ahler
Frank R. Boutillette*
Betty Jo Charles
Richard DelGaudio
Anita Ford*
Scott W. Frew
G. William Graham
Richard Hill
Henry J. Krostich*
Toni Rae T. Lee-Andrews
John J. Lucas
Randy L. Milligan*
J. Clarke Price
Richard W. Reeder*
Jodi L. Rinne
Robert Rohweder
Michael Solakian
Steve Stucky
Randy Watson

**Member—Standards Task Force*

Non-Board Standards Task Force Members
2011 – 2012

Jerry Cross
Heather Reimann

AICPA Staff

Susan S. Coffey
Senior Vice President
Public Practice and Global Alliances

James Brackens, Jr.
Vice President
Ethics and Practice Quality

Gary Freundlich
Technical Director
AICPA Peer Review Program

Susan Lieberum
Senior Technical Manager
AICPA Peer Review Program

Frances McClintock
Senior Technical Manager
AICPA Peer Review Program

Rachelle Drummond
Technical manager
AICPA Peer Review Program

Explanatory Memorandum

Introduction

This memorandum provides background to the proposed changes to the *AICPA Standards for Performing and Reporting on Peer Reviews (Standards*) issued by the AICPA Peer Review Board (Board). The proposed changes would add all examinations performed under the Statements on Standards for Attestation Engagements (SSAE) to the scope of a System Review and Service Organization Control (SOC) 1 and SOC 2 engagements to the types of engagements that must be selected in a System Review.

Background

Scope of System Review

There are two types of peer reviews: System Reviews and Engagement Reviews. System Reviews focus on a firm's system of quality control, and Engagement Reviews focus on work performed on selected engagements. Under current *Standards*, firms that perform engagements under the Statements on Auditing Standards (SASs) or *Government Auditing Standards*, examinations of prospective financial statements or examinations of a service organization's controls likely to be relevant to user entities' internal control over financial reporting (SOC 1 engagements) under SSAEs or audits of non-SEC issuers performed pursuant to the standards of the Public Company Accounting Oversight Board (PCAOB) have System Reviews. Firms that only perform services under Statements on Standards for Accounting and Review Services (SSARS) or services under the SSAEs not included in System Reviews are eligible to have peer reviews called Engagement Reviews.

The Board is proposing to revise the scope of System Reviews to include all examinations performed under SSAEs. The Board considered the similarities between examinations performed under SSAEs and audits performed under SASs, including the requirement in both types of engagements for the practitioner to perform procedures to reduce attestation/audit risk to a level that is appropriately low for a high level of assurance. The Board concluded that the risk of noncompliance by practitioners is the same. Accordingly, all examinations under SSAEs should be included in the scope of a System Review. The Board believes that the inclusion of these engagements in the scope of a System Review will help promote quality in the accounting and auditing services provided by CPA firms and individuals subject to the *Standards*. Although the SSAEs provide for review, agreed-upon procedures, and compilation engagements, the Board does not believe that performing these engagements should require a firm to have a System Review because in these engagements, the practitioner provides either limited assurance (reviews) or no assurance (agreed-upon procedures and compilations).

Must Select Engagements

The *Standards* state that specific types and/or number of engagements must be selected in a System Review. The *Standards* Interpretation 63-1, Office and Engagement Selection in System Reviews, specifies that at least one of each of the following types of engagements is required to be selected for a System Review ("must select" engagements): engagements performed under *Government Auditing Standards*, audits of employee benefit plans, audits subject to Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), and audits of carrying broker-dealers.

The Board considered recommendations from the Information Technology Executive Committee (ITEC) Service Organization Control Reporting Task Force and other research of SOC engagements, as provided in Exhibit A, *SOC Engagements: Background and Other Information Considered.* Based on this research, the Board believes that SOC 1 and SOC 2 engagements should be added to the list of must select engagements. The service auditors' reports resulting from SOC 1 engagements are used by auditors of the financial statements of entities that use service organizations (user entities). SOC 2 reports are used by the management of user entities to obtain information and assurance about the security, availability, processing integrity, confidentiality, or privacy of the systems used by service organizations to process user entity data.

The Board is proposing that SOC 1 and SOC 2 engagements be included in the same pool of engagements for purposes of engagement selection (e.g., if a firm performs three SOC 1 engagements and three SOC 2 engagements, the reviewer is not required to select both a SOC 1 and a SOC 2, selecting a SOC 1 engagement can satisfy the requirement). However, reviewers would be expected to fully document their consideration of all SOC engagements and the basis for their selection in the risk assessment. If a firm performs both SOC 1 and SOC 2 engagements and a proper risk assessment determined that only one SOC engagement should be selected, ordinarily a SOC 1 engagement should be selected over a SOC 2 engagement due to the reliance upon the report by other auditors. Since SOC 2 engagements are a new type of service, peer reviewers may deem it necessary to select both SOC 1 and SOC 2 engagements. However, there may also be situations in which it would be appropriate to pick one SOC 2 and not select a SOC 1. An example may be that the SOC 2 reports have not previously been selected and the SOC 1 reports have, the SOC 2 practice is growing and the SOC 1 practice is stable, etc.

As with other must select engagements, either the team captain or a team member must have at least recent experience (within last 5 years) in the practice area or industry (resume codes A, B, C, or O) to aid in the risk assessment process and determination of which engagements and how many should be selected. While a staff of CPAs may perform SOC 1 engagements, generally SOC 2 engagements would be performed by CPA with IT backgrounds or by a CPA using the work of an IT specialist. Therefore reviews for firms that perform SOC 1 engagements will require a team member with SOC 1 experience. Reviews for firms that perform SOC 2 engagements will require a team member with SOC 2 experience. A team member with experience performing engagements under SSAEs is sufficient for reviews of firms that perform SOC 3 engagements. Due to the specialized nature of SOC engagements, the Board has determined that a specialist may be necessary to assist the team captain in lieu of a team member with SOC experience as described in proposed interpretations 35-1 and 35-2, Qualifying for Service as a Specialist.

The Board believes that making SOC 1 and SOC 2 must select engagements is a proactive revision that will improve the quality of the performance of and reporting on these engagements, and protect the general public. The Board has determined that reviewers should conclude on whether to select SOC 3 engagements based on a proper risk assessment. Refer to Exhibit A, *SOC Engagements: Background and Other Information Considered* for more information.

Impact to Firms Eligible for Engagement Reviews

Interpretation 14-1, Timing of Peer Reviews, states that if a firm, subsequent to the year-end of its Engagement Review, performs an engagement included in paragraph .07 of the *Standards* requiring it to have a System Review, the System Review will be due 18 months after the year-end of the engagement (for financial forecasts and projections: 18 months from the date of report) requiring a System Review or by the firm's next due date, whichever is earlier. The proposed revisions may require firms that have no change to the nature of their practice to be required to have a System Review prior to the firm's next due date. To reduce the burden upon those firms of having two peer reviews in an 18 month period, Interpretation 14-2, Timing of Peer Reviews, was created to provide an exemption to Interpretation 14-1.

Comment Period

The comment period for this exposure draft ends on August 31, 2012.

Written comments on the exposure draft will become part of the public record of the AICPA and will be available on the AICPA's website after October 19, 2012, for a period of one year.

Explanation of Proposed Changes

Revisions to *Standards*

The proposed changes would revise:

- Paragraphs .07, .103, and .104 to include all examinations performed under SSAEs in the scope of a System Review.
- Paragraph .35 to refer to the interpretations.
- Paragraphs .58, .104, and .208, Appendix B, to clarify that attestation engagements are included in the list of engagements subject to peer review based on their period end, not report date, except for financial forecasts or projects.
- Paragraph .207, Appendix A, to explain that SOC 1 and 2 engagements are must selects.
- Paragraph .209, Appendix C, to indicate that a pass report for a System Review should be tailored when SOC engagements are reviewed. The changes in Appendix C would be applied to all of the System Review report examples included in the Appendices to the *Standards*, as applicable.

Revisions to Interpretations

The proposed changes would require changes to:

- Interpretation 8-1, 14-1, and 18-1 to conform to the changes proposed for the *Standards*.
- Interpretations 59-1 and 59-2 regarding the documentation of risk assessment considerations related to SOC engagements.
- Interpretation 63-1 to include service organizations as must select engagements.
- Interpretation 132-1 to include that a national list of consultants with SOC experience will be maintained by the AICPA.

The proposal also includes the creation of the following interpretations:

- Interpretation 7-2 to explain the types of engagements included in the scope of a System Review and an Engagement Review.
- Interpretation 14-2 to explain when firms are exempt from interpretation 14-1.
- Interpretations 35-1 and 35-2 to clarify when and how a specialist may be used on a peer review.

Other changes to the manual, including checklists, will be revised as necessary based on the final guidance approved by the Peer Review Board.

Guide for Respondents

Comments are most helpful when they refer to specific paragraphs, include the reasons for the comments, and, where appropriate, make specific suggestions for any proposed changes to wording.

Comments and responses should be sent to Rachelle Drummond, Technical Manager, AICPA Peer Review Program, AICPA, 220 Leigh Farm Road, Durham, NC 27707-8110 and must be received by August 31, 2012. Respondents can also direct comments and responses to PR_expdraft@aicpa.org by August 31, 2012.

Effective Date

Revisions to the *Standards* adopted as final by the Peer Review Board will be effective for reviews commencing on or after March 1, 2013.

Proposed Revisions

Peer Review Standards

Overview

.07 The objectives of the program are achieved through the performance of peer reviews involving procedures tailored to the size of the firm and the nature of its practice. Firms that perform engagements under the SASs or *Government Auditing Standards,* examinations ~~of prospective financial statements or examinations of a service organization's controls likely to be relevant to user entities' internal control over financial reporting~~ under the SSAEs, or audits of non-SEC issuers performed pursuant to the standards of the PCAOB, as their highest level of service have peer reviews called *System Reviews*. A System Review includes determining whether the firm's system of quality control for its accounting and auditing practice is designed and complied with to provide the firm with reasonable assurance of performing and reporting in conformity with applicable professional standards, including SQCS No. 8, in all material respects. Firms that only perform services under SSARS or services under the SSAEs not included in System Reviews are eligible to have peer reviews called *Engagement Reviews*[1] (see interpretations). Firms that perform audits or play a substantial role in the audit of one or more SEC issuers, as defined by the PCAOB, are required to be registered with and have their accounting and auditing practice applicable to SEC issuers inspected by the PCAOB. Therefore, these standards are not intended for and exclude the review of the firm's accounting and auditing practice applicable to SEC issuers. Firms that do not provide any of the services listed in paragraph 6 are not peer reviewed (see interpretations).

Qualifying for Service as a Peer Reviewer

Other Peer Reviewer or Reviewing Firm Qualification Considerations

.35 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 (see interpretations). For example, computer specialists, statistical sampling specialists, actuaries, or experts in continuing professional education (CPE) may participate in certain segments of the review.

Performing System Reviews

Planning and Performing Compliance Tests
Selection of Engagements

.58 Engagements subject to selection for review ordinarily should be those with periods ending during the year under review, except financial forecasts or projections (see interpretations). ~~For attestation engagements, including financial forecasts or projections, the selection for review ordinarily should be those with report dates during the year under review.~~ Financial forecasts and projections with report dates during the year under review would be subject to selection. If the current year's engagement has not been completed and issued, and if

[1] Although standards no longer permit the performance of Report Reviews as of January 1, 2009, a firm's last peer review could have been a Report Review.

a comparable engagement within the peer review year is not available, the prior year's engagement may be reviewed. If the subsequent year's engagement has been completed and issued, the review team should consider, based on its assessment of peer review risk, whether the more recently completed and issued engagement should be reviewed instead (see interpretations). Review team members should not have contact with or access to any client of the reviewed firm in connection with the peer review.

Performing Engagement Reviews

Objectives

.103 Engagement Reviews are available only to firms that do not perform engagements under the SASs, *Government Auditing Standards*, examinations ~~of prospective financial statements or examinations of a service organization's controls likely to be relevant to user entities' internal control over financial reporting~~ under the SSAEs, or audits of non-SEC issuers performed pursuant to the standards of the PCAOB. However, firms eligible to have an Engagement Review may elect to have a System Review (see interpretations).

Basic Requirements

.104 The criteria for selecting the peer review year-end and the period to be covered by an Engagement Review are the same as those for a System Review (see paragraphs 13–19). Engagements subject to review ordinarily should be those with periods ending during the year under review, except for financial forecasts or projections. ~~For attestation engagements, including financial forecasts or projections, the selection for review ordinarily should be those engagements with report dates during the year under review.~~ Financial forecasts and projections with report dates during the year under review are subject to selection. The reviewed firm should provide summarized information showing the number of its compilation and review engagements performed under SSARS and engagements performed under the SSAEs, classified into industry categories. That information should be provided for each partner, or individual if not a partner, of the firm who is responsible for the issuance of reports on such engagements. On the basis of that information, the review captain or the administering entity ordinarily should select the types of engagements to be submitted for review, in accordance with the following guidelines:

a. One engagement should be selected from each of the following areas of service performed by the firm:

1. Review of historical financial statements (performed under SSARS)
2. Compilation of historical financial statements, with disclosures (performed under SSARS)
3. Compilation of historical financial statements that omits substantially all disclosures (performed under SSARS)
4. Engagements performed under the SSAEs other than examinations ~~of prospective financial statements or examinations of a service organization's controls likely to be relevant to user entities' internal control over financial reporting.~~

b. One engagement should be selected from each partner, or individual of the firm if not a partner, responsible for the issuance of reports listed in item (*a*).

c. Ordinarily, at least two engagements should be selected for review.

.207

Appendix A

Summary of the Nature, Objectives, Scope, Limitations of, and Procedures Performed in System and Engagement Reviews and Quality Control Materials Reviews (as Referred to in a Peer Review Report)

(Effective for Peer Reviews Commencing on or After January 1, 2009)

System Reviews

7. Based on the peer reviewer's planning procedures, the reviewer looks at a sample of the CPA firm's work, individually called engagements. The reviewer selects engagements for the period covered by the review from a cross section of the firm's practice with emphasis on higher risk engagements. The engagements selected include those performed under *Government Auditing Standards*, audits of employee benefit plans, audits of depository institutions (with assets of $500 million or greater), ~~and~~ audits of carrying broker-dealers, and examinations of service organizations (Service Organization Control [SOC] 1 and 2 engagements) when applicable. The scope of a peer review only covers accounting and auditing engagements performed under U.S. professional standards; it does not include the firm's SEC issuer practice, nor does it include tax or consulting services. The reviewer will also look at administrative elements of the firm's practice to test the elements listed previously from the Statements on Quality Control Standards.

.208

Appendix B

Considerations and Illustrations of Firm Representations

1. The team captain or review captain obtains written representations from management of the reviewed firm to describe matters significant to the peer review in order to assist in the planning and performance of and the reporting on the peer review. In connection with System and Engagement Reviews, specific representations should relate to the following matters, although the firm is not prohibited from making additional representations, and the firm may tailor the representation letter as it deems appropriate, as long as the minimum applicable representations are made to the team captain or review captain (see interpretations):

a. Situations or a summary of situations where management is aware that the firm or its personnel has not complied with the rules and regulations of state board(s) of accountancy or other regulatory bodies (including applicable firm and individual licensing requirements in each state in which it practices for the year under review) and, if applicable, how the firm has or is addressing and rectifying situations of noncompliance (see interpretations).

b. Communications or summary of communications from regulatory, monitoring, or enforcement bodies relating to allegations or investigations of deficiencies in the conduct of an accounting, audit, or attestation engagement performed and reported on by the firm, whether the matter relates to the firm or its personnel, within the three years preceding the firm's current peer review year-end and through the date of the exit conference. The information should be obtained in sufficient detail to consider its effect on the scope of the peer review (see interpretations). In addition, the reviewer may inquire if there are any other issues that may affect the firm's practice.

c. Restrictions or limitations on the firm's or its personnel's ability to practice public accounting by regulatory, monitoring, or enforcement bodies within three years preceding the current peer review year-end.

d. Completeness and availability of the engagements with periods ending during the year under review, except financial forecasts and projections. ~~For engagements performed under the Statements on Standards for Attestation Engagements, including f~~Financial forecasts and projections~~, this includes those~~ with report dates during the year under review~~.~~ would be subject to selection.

e. Discussions of significant issues from reports or communications, or both (see interpretations), from other practice monitoring or external inspection programs, such as the Public Company Accounting Oversight Board's (PCAOB's) (see interpretations), with the team captain.

f. Accepting responsibility for understanding, tailoring, and augmenting the quality control materials that the firm develops or adopts for use in its accounting and auditing practice.

g. Other representations obtained by the team captain or review captain will depend on the circumstances and nature of the peer review.

2. The written representations should be obtained for the entire firm and not for each individual engagement the firm performs. Firm management's refusal to furnish written representations to the team captain or review captain constitutes a failure to cooperate with the reviewer and thus the administering entity and with the AICPA Peer Review Board, and the firm

would be subject to fair procedures that could result in the firm's enrollment in the program being terminated (see interpretations).

3. On System Reviews, the written representations should be addressed to the team captain. Since the team captain is concerned with events occurring during the peer review period and through the date of his or her peer review report that may require an adjustment to the report or other peer review documents, the representations should be dated the same date as the peer review report. The written representations should be signed by those members of management whom the team captain believes are responsible for and knowledgeable about, directly or through others in the firm, the matters covered in the representations, the firm, and its system of quality control. Such members of management normally include the managing partner and partner or manager in charge of the firm's system of quality control. If a representation made by management is contradicted by other information obtained, the team captain should investigate the circumstances and consider the reliability of the representations made and any effect on the report.

4. On Engagement Reviews, the representations should be addressed to the review captain (for example, "To John Smith, CPA" or on committee-appointed review team reviews where appropriate, it may be addressed "To the Review Captain") and dated the same date that the firm submits the list of engagements to the reviewer or the administering entity. The written representations should be signed by those members of management whom the reviewer or the administering entity believes are responsible for and knowledgeable about, directly or through others in the firm, the matters covered in the representations, the firm, and its system of quality control (even though an Engagement Review). Such members of management normally include the managing partner and partner or manager in charge of the firm's system of quality control. If a representation made by management is contradicted by other information obtained, the reviewer should investigate the circumstances and consider the reliability of the representations made and any effect on the report.

Illustration of a Representation Letter That has No Significant Matters to Report to the Team Captain or Review Captain

(The firm may tailor the language in this illustration and may refer to attachments to the letter as long as adequate representations pertaining to the matters discussed above, as applicable, are included to the satisfaction of the team captain or review captain.)

October 31, 20XX

To the Team Captain or Review Captain

We are providing this letter in connection with the peer review of [name of firm] as of the date of this letter and for the year ended June 30, 20XX.

We understand that we are responsible for complying with the rules and regulations of state boards of accountancy and other regulators. We confirm, to the best of our knowledge and belief, that there are no known situations in which [name of firm] or its personnel have not complied with the rules and regulations of state board(s) of accountancy or other regulatory bodies, including applicable firm and individual licensing requirements in each state in which it practices for the year under review. We have also provided a list of all engagements to the [team captain, review captain, or administering entity] with periods ending during the year under review. For ~~attestation engagements, including~~ financial forecasts or projections, the list included those engagements with report dates during the year under review. We have also provided the [team captain or review captain] with any other information requested, including communications by regulatory, monitoring, or enforcement bodies relating to allegations or investigations in the conduct of its accounting, audit, or attestation engagements performed and reported on by the firm, whether the matter relates to the firm or its personnel, within three years preceding the current peer review year-end. In addition, there are no known restrictions or limitations on the firm's or its personnel's ability to practice public accounting by regulatory, monitoring, or enforcement bodies within three years preceding the current peer review year-end. We understand the intended uses and limitations of the quality control materials we have developed or adopted. We have tailored and augmented the materials as appropriate such that the quality control materials encompass guidance which is sufficient to assist us in conforming with professional standards (including the Statements on Quality Control Standards) applicable to our accounting and auditing practice in all material respects. We have also discussed the content of our PCAOB inspection report with the [team captain or review captain] (if applicable).

Sincerely,

[*Name of reviewed firm*]

Illustration of a Representation Letter That Has Been Tailored to Report to the Team Captain a Matter of Noncompliance With a Regulatory Requirement

(The firm may tailor the language in this illustration and may refer to attachments to the letter as long as adequate representations pertaining to the matters discussed above, as applicable, are included to the satisfaction of the team captain or review captain.)

October 31, 20XX

To the Team Captain or Review Captain

We are providing this letter in connection with the peer review of [name of firm] as of the date of this letter and for the year ended June 30, 20XX.

We understand that we are responsible for complying with the rules and regulations of state boards of accountancy and other regulators. Other than the firm not having a practice unit license during the year under review in one state where the firm practices (which has been subsequently obtained), we confirm, to the best of our knowledge and belief, that there are no known situations in which [name of firm] or its personnel have not complied with the rules and regulations of state board(s) of accountancy or other regulatory bodies, including applicable firm and individual licensing requirements in each state in which it practices for the year under review. We have also provided a list of all engagements to the [team captain, review captain, or administering entity] with periods ending during the year under review. For ~~attestation engagements, including~~ financial forecasts or projections, the list included those engagements with report dates during the year under review. We have also provided the [team captain] with any other information requested, including communications by regulatory, monitoring, or enforcement bodies relating to allegations or investigations in the conduct of its accounting, audit, or attestation engagements performed and reported on by the firm, whether the matter relates to the firm or its personnel, within three years preceding the current peer review year-end. In addition, there are no known restrictions or limitations on the firm's or its personnel's ability to practice public accounting within three years preceding the current peer review year-end. We understand the intended uses and limitations of the quality control materials we have developed or adopted. We have tailored and augmented the materials as appropriate such that the quality control materials encompass guidance which is sufficient to assist us in conforming with professional standards (including the Statements on Quality Control Standards) applicable to our accounting and auditing practice in all material respects. We have also discussed the content of our Public Company Accounting Oversight Board inspection report with the team captain (if applicable).

Sincerely,

[*Name of reviewed firm*]

.209

Appendix C

Illustration of a Report With a Peer Review Rating of *Pass* in a System Review

[*Firm letterhead for a firm-on-firm review; team captain's firm letterhead for an association formed review team*.]

System Review Report

October 31, 20XX

To the Partners of [*or other appropriate terminology*]
XYZ & Co.
and the Peer Review Committee of the [*insert the name of the applicable administering entity*][2]

We[3] have reviewed the system of quality control for the accounting and auditing practice of XYZ & Co. (the firm)[4] in effect for the year ended June 30, 20XX. Our peer review was conducted in accordance with the Standards for Performing and Reporting on Peer Reviews established by the Peer Review Board of the American Institute of Certified Public Accountants. The firm is responsible for designing a system of quality control and complying with it to provide the firm with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Our responsibility is to express an opinion on the design of the system of quality control and the firm's compliance therewith based on our review. The nature, objectives, scope, limitations of, and the procedures performed in a System Review are described in the standards at www.aicpa.org/prsummary.

As required by the standards, engagements selected for review included (engagements performed under *Government Auditing Standards*; audits of employee benefit plans, audits performed under FDICIA, ~~and~~ audits of carrying broker-dealers, and examinations of service organizations [Service Organizations Control (SOC) 1 and 2 engagements].)[5]

In our opinion, the system of quality control for the accounting and auditing practice of XYZ &

---

[2] The report of a firm whose review is administered by the National Peer Review Committee should be addressed as follows: To the Partners of [or appropriate terminology] XYZ & Co. and the National Peer Review Committee.

[3] The report should use the plural *we, us*, and *our* even if the review team consists of only one person. The singular *I, me*, and *my* are appropriate only if the reviewed firm has engaged another firm to perform its review and the reviewing firm is a sole practitioner.

[4] The report of a firm who is required to be registered and inspected by the PCAOB and thus whose review is administered by the National Peer Review Committee should be tailored here to add "applicable to non-SEC issuers."

[5] If the firm performs audits of employee benefit plans, engagements performed under *Government Auditing Standards*, audits of depository institutions with total assets of $500 million or greater at the beginning of its fiscal year, audits of carrying broker-dealers, examinations of service organizations (Service Organization Control [SOC] 1 and SOC 2), or other engagements required to be selected by the board in interpretations, the engagement type(s) selected for review should be identified in the report using this paragraph, tailored as applicable. For SOC engagements, the paragraph should be tailored to reflect the type(s) selected for review. If the firm does not perform such engagements, this paragraph is not applicable and not included in the report.

Co.[6] in effect for the year ended June 30, 20XX, has been suitably designed and complied with to provide the firm with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Firms can receive a rating of *pass*, *pass with deficiency(ies)* or *fail*. XYZ & Co. has received a peer review rating of *pass*.

Smith, Jones and Associates

[*Name of team captain's firm*]

[6] The report of a firm who is required to be registered and inspected by the PCAOB and thus whose review is administered by the National Peer Review Committee should be tailored here to add "applicable to non-SEC issuers."

Peer Review Standards Interpretations

Engagements Under Peer Review

7-2 *Question*—Paragraph .07 of the standards indicates that firms that perform engagements under the SASs or *Government Auditing Standards,* examinations under the SSAEs, or audits of non-SEC issuers performed pursuant to the standards of the PCAOB have peer reviews called *System Reviews*. Firms that only perform services under SSARS or services under the SSAEs not included in System Reviews have peer reviews called *Engagement Reviews*. Is the System Review or Engagement Review determination based on the types of engagements a firm performs as its highest level of service?

Interpretation— Yes. The type of peer review determination is made based on the engagements performed as its highest level of service.

If a Firm Performs These Types of Engagements as Its Highest Level of Service, the Firm Would be Required to Have:	System Review	Engagement Review
Statements on Auditing Standards (SAS)		
Audits	X	
Government Auditing Standards (GAS)		
Audits	X	
Statements on Standards for Attestation Engagements (SSAEs)		
Examinations performed under AT section 101, *Attest Engagements* (AICPA, *Professional Standards*)	X	
Reviews performed under AT section 101		X
Agreed-upon procedures performed under AT section 201, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*)		X
Examinations of prospective financial statements performed under AT section 301, *Financial Forecasts and Projections* (AICPA, *Professional Standards*)	X	
Compilations of prospective financial statements and application of agreed-upon procedures to prospective financial statements performed under AT section 301		X
Examinations performed under AT section 401, *Reporting on Pro Forma Financial Information* (AICPA, *Professional Standards*)	X	
Reviews performed under AT section 401		X
Examinations performed under AT section 501, *An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements* (AICPA, *Professional Standards*)	X	

Examinations performed under AT section 601, *Compliance Attestation* (AICPA, *Professional Standards*)	X	
Agreed-upon procedures performed under AT section 601		X
Examinations performed under AT section 701, *Management's Discussion and Analysis* (AICPA, *Professional Standards*)	X	
Reviews performed under AT section 701		X
Examinations performed under AT section 801, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*)	X	
Public Company Accounting Oversight Board (PCAOB) Standards		
Audits	X	
Statements on Standards for Accounting and Review Services (SSARS)		
Reviews of financial services		X
Compilations of financial statements with disclosures		X
Compilations of financial statements without disclosures		X
Compilations performed when the compiled financial statements are not expected to be used by a third party (management use only), when no compilation report Is issued[7]		X

If a firm is required to have a System Review, all the engagements previously listed would be subject to selection for review, ordinarily based on periods ending during the year under review, except for financial forecasts and projections. Financial forecasts and projections with report dates during the year under review would be subject to selection.

If a firm performs or reports on engagements under International Standards, refer to Interpretations 6-7 and 6-8.

Performing System Reviews at a Location Other Than the Reviewed Firm's Office

8-1 *Question*—Paragraph .08 of the standards states that the majority of the procedures in a System Review should be performed at the reviewed firm's office. What criteria have been established by the board for procedures to be performed at a location other than the reviewed firm's office?

Interpretation—If the review can reasonably be performed at the reviewed firm's office, it should be. Although certain planning procedures may be performed at the peer reviewer's office, it is expected that a majority of the peer review procedures,

[7] Refer to Interpretations 6-1 to 6-6.

including the review of engagements, testing of functional areas, interviews, and concluding procedures should be performed at the reviewed firm's office.

However, it is recognized that there are some situations that make an on-site peer review cost prohibitive or extremely difficult to arrange, or both. In these situations, if the firm and reviewer mutually agree on the appropriateness and efficiency of an approach to the peer review such that it can be performed at a location other than the reviewed firm's office, then the reviewer can request the administering entity's approval to perform the review at a location other than the reviewed firm's office. This request should be made prior to the commencement of fieldwork, and the firm and reviewer should be prepared to respond to the administering entity's inquiries about various factors that could affect their determination. These factors, which are not mutually exclusive and will be considered judgmentally, include but are not limited to

- the availability of peer reviewers qualified to review the firm, including whether they have the experience in the industries and related levels of service for which the firm practices, whether they are independent of the firm and not, for instance, competitors within the same close geographic area, and whether the firm is reasonably accessible to those reviewers.
- whether the review conducted at the reviewer's office or another agreed-upon location can still achieve the objectives of a System Review.
- whether the results are expected to be the same as they would be if the peer review was performed at the reviewed firm's office.
- the size of the reviewed firm, including the number of personnel and where they perform their work (for instance, whether they work solely at clients' offices and the firm does not have its own office).
- the number of engagements covered by the Statements on Auditing Standards (SASs), *Government Auditing Standards*, examinations ~~of prospective financial statements or examinations of a service organization's controls likely to be relevant to user entities' internal control over financial reporting~~ under the Statements on Standards for Attestation Engagements (SSAEs), or audits of non-Securities and Exchange Commission (SEC) issuers performed pursuant to the standards of the Public Company Accounting Oversight Board (PCAOB).
- the ability of the reviewed firm and the peer reviewer to hold one or more effective meetings by telephone to discuss the firm's responses to the quality control policies and procedures questionnaire and other practice aid questionnaires (including various interviews), Engagement Review results, the reviewer's conclusions on the peer review, and any recommended corrective actions.
- the prior peer review results of the firm, including whether the firm received a report with a peer review rating of *pass with deficiencies* or *fail* (formerly known as modified or adverse reports) on its last System or Engagement Review (or a report review with significant comments), or if it is the firm's first System Review.

- whether the firm is able to effectively comply with the reviewer's requests for materials to be sent to the reviewer prior to the review (except as noted in the following list). Those requests should include, in addition to materials outlined in section 4100, *Instructions to Firms Having a System Review*, the following materials:

    a. All documentation related to the resolution of independence questions (1) identified during the year under review with respect to any audit or accounting client or (2) related to any of the audit or accounting clients selected for review, no matter when the question was identified if the matter still exists during the review period

    b. The most recent independence confirmations received from other firms of CPAs engaged to perform segments of engagements on which the firm acted as principal auditor or accountant

    c. The most recent representations received from the sole practitioner concerning his or her conformity with applicable independence requirements

    d. A written representation, dated the same as the peer review report, as described in paragraph .05(f) and appendix B of the standards

    e. Documentation, if any, of consultations with outside parties during the year under review in connection with audit or accounting services provided to any client

    f. A list of relevant technical publications used as research materials, as referred to in the quality control policies and procedures questionnaire

    g. A list of audit and accounting materials, if any, identified in response to the questions in the "Engagement Performance" section of the quality control policies and procedures questionnaire

    h. Continuing professional education (CPE) records sufficient to demonstrate compliance with state, AICPA, and other regulatory CPE requirements

    i. The relevant accounting and auditing documentation and reports on the engagements selected for review

    j. Documentation of the firm's monitoring results for each year since the last peer review or enrollment in the program

    k. Any other evidential matter requested by the reviewer

The reviewed firm should understand that in the event that matters are noted during the review of selected engagements, the scope of the review may have to be expanded before the review can be concluded.

Timing of Peer Reviews

14-1 *Question*—Paragraph .14 of the standards states that when a firm performs its first engagement requiring it to have a System Review, the firm's next due date will be 18 months from the year-end of the engagement. What does this mean?

Interpretation—When a firm, subsequent to the year-end of its ~~Report or~~ Engagement Review, performs an engagement under the SASs, *Government Auditing Standards*, examinations ~~of prospective financial statements or examinations of a service organization's controls likely to be relevant to user entities' internal control over financial reporting~~ under the SSAEs, or an audit of a non-SEC issuer performed pursuant to the standards of the PCAOB that would have required the firm to have a System Review, the firm should (*a*) immediately notify the administering entity and (*b*) undergo a System Review. The System Review ordinarily will be due 18 months from the year-end of the engagement (for financial forecasts and projections: 18 months from the date of report) requiring a System Review or by the firm's next scheduled due date, whichever is earlier. However, the administering entity will consider the firm's practice, the year-ends of engagements and when the procedures were performed, and the number of engagements to be encompassed in the review, as well as use its judgment, to determine the appropriate year-end and due date. Firms that fail to immediately inform the administering entity of the performance of an engagement previously described will be required to participate in a System Review with a peer review year-end that covers the engagement. A firm's subsequent peer review ordinarily will be due 3 years and 6 months from this peer review year-end.

14-2 *Question*—When a firm has been performing engagements that allowed it to have an Engagement Review and, as a result of a change in paragraph .07 of the standards is now required to have a System Review, is the firm's next due date 18 months from the year-end of the engagement (report date for financial forecasts and projects) triggering a System Review?

Interpretation—No. If the firm continues to only perform the types of engagements that previously allowed it to have an Engagement Review, the firm would not be required to have its next peer review due 18 months from the year-end of the engagement (or report date for financial forecasts and projects) triggering a System Review. The firm will stay on its current peer review cycle and the type of review for its next peer review will be determined based on the date it is scheduled. A firm's review is defined as scheduled when the review team is approved by the administering entity.

- If a review is scheduled prior to the effective date of the change to paragraph .07 of the standards and commences within one year of being scheduled, the firm may still have an Engagement Review or elect to have a System Review.
- If a review is scheduled prior to the effective date of the change to paragraph .07 of the standards, but does not commence within one year, the firm will have a System Review.
- If a review (regardless of commencement date) is scheduled on or after the effective date of the change to paragraph .07 of the standards, the firm will have a System Review.

For each scenario, the firm's subsequent peer review will be a System Review, ordinarily due 3 years and 6 months from the year-end of the peer review described above.

18-1 *Question*—Paragraph .18 of the standards requires that a firm maintain the same year-end on subsequent peer reviews (which is 3 years from the previous year-end) and the same review due date (which is 3 years from the previous due date). What options does a firm have to change its year-end or extend the due date?

Interpretation—A firm is expected to maintain the same year-end on subsequent peer reviews. Nevertheless, circumstances may arise that may influence a firm to want to change its year-end. For instance, the nature of the firm's practice may change or they may reevaluate their current year-end and determine as a result that a different year-end is more practical. In such situations, a firm may change its year-end only with prior, written approval of the administering entity.

Administering entities will consider many factors including the nature of the firm's practice (for instance, when audits are being performed and issued so they will be available for the peer review, tax season, and so on). However, a change in year-end will usually not be approved when there is a public interest concern. This may occur when the firm is requesting the change in an attempt to have an Engagement Review, rather than a System Review, or when a change in year-end would cause the firm's only engagement meeting the criteria described in Interpretation 63-1~~,~~ (engagements conducted in accordance with *Government Auditing Standards* [GAS, also known as the Yellow Book]; audits conducted pursuant to the Employee Retirement Income Security Act of 1974 (ERISA); audits of an insured depository institution subject to the FDIC Improvement Act of 1991; ~~or~~ audits of carrying broker-dealers; or examinations of service organizations (Service Organization Control [SOC] 1 and 2 engagements) to fall out of the peer review selection process.

Ordinarily, the firm's due date for the subsequent peer review will be three years and six months from the year-end of the current peer review.

A firm is expected to maintain the same review due date. Nevertheless, circumstances may arise that require the firm to extend its review due date. In such situations, a firm may do so only with prior, written approval of the administering entity, and the extended review due date only applies to the current review. Extensions for subsequent review's due dates must be reapplied for.

Extensions of a review due date by more than three months should be rare. However, in some situations, due to the size of the firm, the complexity of the peer review, and whether or not the review team is integrating peer review procedures with the firm's internal inspection procedures, it is not unusual for a peer review to occur over a number of months. In such situations, a firm whose peer review has oversight performed by the administering entity may extend its review due date by up to six months with prior, written approval of the administering entity.

In any of the situations previously described, it is the responsibility of the firm to ensure that any change in the review due date (or year-end) approved by the administering entity is recognized by any other organizations requiring it to have a

peer review. This includes but is not limited to state boards of accountancy, the Government Accountability Office, and other regulators.

Qualifying for Service as a Specialist

35-1 *Question*—Paragraph .35 of the standards states that 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. At what point is a specialist going beyond a consulting capacity on the peer review?

Interpretation—The specialist is going beyond a consulting capacity when he or she prepares any other peer review documentation beyond preparing and completing the engagement checklist and Matter for Further Consideration (MFC) forms. When MFC forms are prepared for the engagement the specialist is reviewing, the specialist should plan on being available during the exit conference.

35-2 *Question*—If a review team uses a specialist to prepare and complete the engagement checklist and MFC forms for a must select engagement as described in interpretation 63-1, is another team member required to have experience with the must select industry?

Interpretation—Yes. An approved team member with the appropriate experience is required to review all must select engagements except service organization control (SOC 1 and 2) engagements. A specialist meeting criteria established by the AICPA may be approved to assist the team in reviewing SOC 1 or SOC 2 engagements. The firm is required to obtain approval from its administering entity if it will be using a specialist instead of a team member with SOC 1 or SOC 2 experience. A list of preapproved specialists will be maintained by the AICPA.

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 administering entity, preparing the report on the review, and ensuring that peer review documentation is complete and submitted to the administering entity 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.

Office and Engagement Selection in System Reviews

59-1 *Question*—Paragraph .59 of the standards requires that engagements selected for review should provide a reasonable cross section of the reviewed firm's accounting and auditing practice, with greater emphasis on those engagements in the practice with higher assessed levels of peer review risk, and the guidance provides examples of factors to consider when assessing peer review risk at the engagement level. What are some other considerations?

Interpretation—A reasonable cross section of a firm's accounting and auditing practice, not only includes consideration of the specific industries that are required to be selected, but other industries that have a significant public interest. Industries that have a significant public interest are those that benefit the general welfare of

the public, such as those that have recent regulatory and legislative developments (for example broker-dealers). Public interest industries will vary across firms and reviewers should consider the composition of a firm's accounting and auditing practice when determining if their risk assessment should address a public interest industry. The reviewer also needs to carefully consider the industries that the firm has identified in the category of "other audits" when determining whether to select such an engagement(s). A selection consisting solely of public interest industries would not necessarily represent a reasonable cross section. Other factors to consider in selecting a reasonable cross section may include the number of partners, the number of practice offices, and materiality thresholds of accounting and auditing hours.

The reviewer should explain and document in the *Summary Review Memorandum* key decisions that he or she made when he or she chose not to select any one or more of the following: a level of service, industries in which a significant public interest exists, and industries in which the firm performs a significant number of engagements. This does not give authority to the reviewer to avoid selecting an engagement(s) by simply documenting the reason(s) why he or she did not select certain engagement(s). Therefore the reviewer should document important considerations regarding the engagement selection process.

A reasonable cross section does not always require that at least one engagement from every level of service provided by the firm be selected for review; however, it often may be appropriate in the circumstances. There is no percentage of coverage that necessarily ensures a reasonable cross section. Therefore, there is a relationship between a risk-based approach and a reasonable cross section when selecting engagements, and in that regard each peer review needs to be considered on a case-by-case basis.

The following are examples of risk considerations when addressing obtaining a reasonable cross section of the engagements, including engagements that must be selected and non-carrying broker-dealers. It is expected that the various types of engagements within an industry are specifically addressed in the risk assessment. Similar considerations should be made for industries that have a significant public interest.

a. *Governmental—Government Auditing Standards*—Inclusion of a must select engagement should not supersede the reviewer's consideration of engagements and industries that have a significant public interest such as state and local governments, school districts and HUD engagements. For example, if for-profit HUD multi-family housing project audit engagements constitute a significant percentage of a firm's practice, one would expect the reviewer to select at least one such engagement for review. However, if the firm also performed an audit of an engagement subject to Circular A-133, such as a local government or not-for-profit organization, one such engagement must also be selected to perform an evaluation of the firm's compliance with Circular A-133. Peer reviewers should also consider audit firm experience such as how many governmental audits the firm performs, the length of experience in performing these engagements, the size of the audit firm, the number of team members with experience, and whether the team members

have undergone CPE or specialized training. Further consideration should be given to communications from regulatory agencies.

b. *Employee benefit plans*—For employee benefit plans under ERISA, the peer reviewer should consider whether the engagement selection process has adequately addressed the risks involved in limited versus full scope audits and in different types of benefit plans such as defined benefit, defined contribution, and voluntary health and welfare plans. If a firm has more than one of the preceding types of plans, the reviewer must consider the unique risks associated with that type of plan and document how these risks were addressed in the risk assessment. Peer reviewers should also consider audit firm experience such as how many ERISA audits the firm performs, the length of experience in performing these engagements, the size of the audit firm, the number of team members with experience, and whether the team members have undergone CPE or specialized training. Further consideration should be given to communications from regulatory agencies.

c. *Depository Institutions*—For FDICIA engagements, peer reviewers should take into consideration the amount of total assets held by the federally insured depository institution (less than $500 million, more than $500 million, more than $1 billion). Peer reviewers should also consider audit firm experience such as how many FDICIA audits the firm performs, the length of experience in performing these engagements, the size of the audit firm, the number of team members with experience, and whether the team members have undergone CPE or specialized training. Further consideration should be given to the risks of the audited company such as the level of reporting the institution complies with (the holding company level or the bank subsidiary level and the regulatory issues associated with each), the balance of the lending portfolio (the industries and concentration percentage of the portfolio), any regulatory correspondence and examination results, capital ratios, financial institution management experience, economic environment and geographic location of the institution, number of branches, and experience and longevity of the board of directors and audit committee.

d. *Broker-dealers*—The peer reviewer should consider whether the engagement selection process has adequately addressed the risks involved in carrying and non-carrying broker-dealers. Consideration of carrying broker-dealers should include carrying, clearing, and custodial broker-dealers. Consideration of non-carrying broker-dealers should include introducing broker-dealers. The peer reviewer should also consider other types of broker-dealers that fit the description of carrying and non-carrying broker-dealers in Interpretation No. 63-2. If a firm has more than one of the preceding types of audits, the reviewer must consider the unique risks associated with that type of audit and document how these risks were addressed in the risk assessment. For all broker-dealer engagements, the peer reviewer should consider audit firm experience such as how many broker-dealer audits the firm performs, the length of experience in performing these engagements, the size of the audit firm, team members with experience, and CPE or specialized training. Further consideration should be given to communications from regulatory agencies. For non-carrying broker-dealers, the peer reviewer's risk assessment is expected to address the risks associated with those broker-dealers (for

example, if the broker-dealer has some form of custody and control that may create risk and require additional internal controls).

e. Service Organizations—The peer reviewer should consider whether the engagement selection process has adequately addressed the risks involved in different types of Service Organization Control (SOC) engagements (SOC 1 and 2 engagements). If a firm performs more than one of the preceding types of SOC engagements, the reviewer must consider the unique risks associated with that type of engagement and document how these risks were addressed in the risk assessment. Peer reviewers should also consider audit firm experience such as how many SOC engagements the firm performs, the length of experience in performing these engagements, the size of the audit firm, the number of team members with experience, and reasonableness of fees charged for SOC engagements, and whether the team members have undergone CPE or specialized training. Further consideration should be given to communications from regulatory agencies. Similar considerations should be made for SOC 3 engagements.

59-2 *Question*—Paragraph .59 of the standards provides factors to consider when assessing peer review risk at the engagement level. What are some other examples of factors to consider?

Interpretation—Other examples of factors to consider when assessing peer review risk at the engagement level follow. This list is for illustrative purposes only, and does not include all possible inherent and control risk factors, nor is the peer reviewer required to consider every item on the list when assessing inherent and control risk:

- Engagement size, in terms of the hours required to plan and perform it
- Engagements involving experienced personnel hired from other firms, and partners who also have office, regional or firm-wide management, administrative, or functional responsibilities
- Engagements where work on segments has been referred to other firms, foreign offices, domestic or foreign affiliates, or correspondents
- Engagements where one or more affiliated entities (for example, parent companies and subsidiaries or brother and sister companies) constitute a large portion of the firm's overall clientele
- Engagements identified in the firm's quality control System or guidance material as having a high degree of risk
- Engagements where departures from professional standards and failure to comply with the firm's quality control policies and procedures were noted in the preceding year's monitoring procedures
- Engagements in industries where the firm has experienced high instances of litigation, proceedings, or investigations
- Engagements affected by recently implemented revisions of the firm's quality control policies and procedures
- Engagements affected by newly effective professional standards
- Clients in industries in poor financial condition

- Clients in industries with complex or sophisticated transactions
- Engagements from merged-in practices
- Engagements subject to *Government Auditing Standards*
- Engagements subject to the Employee Retirement Income Security Act of 1974 (ERISA)
- Engagements subject to the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA)
- Audits of securities and commodities broker-dealers
- Examinations of controls relevant to both a service organization and its user entities

63-1 *Question*—Paragraph .63 of the standards requires that specific types or number of engagements must be selected in a System Review as well as specific audit areas. In a System Review, what specific types and number of engagements, if any, should be included in the sample of engagements selected for review or assessed at a higher level of peer review risk?

Interpretation—At least one of each of the following types of engagements is required to be selected for review in a System Review:

a. Governmental—Government Auditing Standards, issued by the U.S. Government Accountability Office, requires auditors conducting engagements in accordance with those standards to have a peer review that includes the review of at least one engagement conducted in accordance with those standards. If a firm performs an engagement of an entity subject to GAS and the peer review is intended to meet the requirements of those standards, at least one engagement conducted pursuant to those standards should be selected for review. Additionally, if the engagement selected is of an entity subject to GAS but not subject to the Single Audit Act/OMB Circular A-133 and the firm performs engagements of entities subject to OMB Circular A-133, at least one such engagement should also be selected for review. The review of this additional engagement must evaluate the compliance audit requirements and may exclude those audit procedures strictly related to the audit of the financial statements.

b. Employee Benefit Plans—Regulatory and legislative developments have made it clear that there is a significant public interest in, and a higher risk associated with, audits conducted pursuant to ERISA. Therefore, if a firm performs the audit of one or more entities subject to ERISA, at least one such audit engagement conducted pursuant to ERISA should be selected for review.

c. Depository Institutions—The 1993 FDIC guidelines implementing the FDICIA require auditors of federally insured depository institutions having total assets of $500 million or greater at the beginning of its fiscal year to have a peer review that includes the review of at least one audit of an insured depository institution subject to the FDICIA. If a firm performs an audit of a federally insured depository institution subject to the FDICIA and the peer review is intended to meet the requirements of the FDICIA, at least one engagement

conducted pursuant to the FDICIA should be selected for review. The review of that engagement should also include a review of the reports on internal control if applicable because those reports are required to be issued under the FDICIA when total assets exceed $1 billion.

d. *Broker-Dealers*—Regulatory and legislative developments have made it clear that there is a significant public interest in, and a higher risk associated with, audits of broker-dealers. The type of broker-dealer with the highest risk is a carrying broker-dealer. Therefore, if a firm performs the audit of one or more carrying broker-dealers, at least one such audit engagement should be selected for review. It is also expected that if a firm's audits of broker-dealers include only non-carrying broker-dealers, the team captain should be aware of and give special consideration to the risks associated with such broker-dealer audits in making engagement selections.

e. *Service Organizations*—Due to the reliance on Service Organization Control (SOC) reports, particularly SOC 1 and 2 reports, there is a significant public interest in examinations of service organizations relevant to user entities. Therefore, if a firm performs an examination of one or more service organizations and issues a SOC 1 or SOC 2 report, at least one such engagement should be selected for review. If a firm performs both SOC 1 and SOC 2 engagements and a proper risk assessment determined that only one SOC engagement should be selected, ordinarily a SOC 1 engagement should be selected over a SOC 2 engagement due to the reliance upon the report by other auditors. Because SOC 2 engagements are a new type of service, peer reviewers may deem it necessary to select both SOC 1 and SOC 2 engagements. However, there may also be situations in which it would be appropriate to pick one SOC 2 and not select a SOC 1. An example may be that the SOC 2 reports have not previously been selected and the SOC 1 reports have been selected; the SOC 2 practice is growing and the SOC 1 practice is stable; and so on.

In complying with the requirements in the previous list, peer reviewers should also ensure that the engagements selected include a reasonable cross section of the firm's accounting and auditing engagements, appropriately weighted considering risk. Thus, the peer reviewer may need to select greater than the minimum of one engagement from these industries in order to attain this risk weighted cross section. Refer to Interpretation 59-1.

~~For benefit plans under ERISA, the peer reviewer should also consider whether the engagement selection process has adequately addressed the risks involved in limited versus full scope audits and in different types of benefit plans such as defined benefit, defined contribution, and voluntary health and welfare plans. Similar considerations should be made on GAS, FDICIA, and broker-dealer engagements.~~

The team captain's consideration of this coverage should be discussed in his or her risk assessment documentation. This discussion should include any factors considered when the reviewed firm has a significant number of engagements in one of these high risk areas and it is not otherwise evident why only one engagement from the industry has been included in the scope of the review.

Election to Have a System Review

103-1 *Question*—Paragraph .103 of the standards notes that firms eligible to have an Engagement Review may elect to have a System Review. What ~~modifications are~~tailoring is required to the peer review report under these circumstances?

Interpretation—Under these circumstances, any references in the peer review report to "the accounting and auditing practice" should be ~~modified~~ tailored to refer only to "the accounting practice." In addition, the sentence "Firm XYZ & Co. has represented to us that the firm performed no services under the SASs; *Government Auditing Standards*; examinations ~~of prospective financial statements or examinations of a service organization's controls likely to be relevant to user entities' internal control over financial reporting~~ under the Statements on Standards for Attestation Engagements (SSAEs); or audits of non-SEC issuers performed pursuant to the standards of the Public Company Accounting Oversight Board (PCAOB)" should be added.

Qualifying for Service as a Peer Review Committee Member, Report Acceptance Body Member, or Technical Reviewer

132-1 *Question*—Paragraphs .132 and .136 of the standards note that minimum requirements must be met to be a peer review committee member, a report acceptance body member, or a technical reviewer. What are those requirements?

Interpretation—
Peer Review Committee Member
A majority of the peer review committee members and the chairperson charged with the overall responsibility for administering the program at the administering entity should possess the qualifications required of a team captain in a System Review. A committee member who is suspended or restricted from scheduling or performing peer reviews no longer meets the qualifications until such suspension or restriction is removed. Reinstatement as a committee member would be at the discretion of the administering entity or committee.

Report Acceptance Body Member
Each member of an administering entity's report acceptance body charged with the responsibility for acceptance of peer reviews should

a. be currently active in public practice at a supervisory level in the accounting or auditing function of a firm enrolled in the program, as a partner of the firm, or as a manager or person with equivalent supervisory responsibilities. To be considered currently active in the accounting or auditing function, a reviewer should be presently involved in the accounting or auditing practice of a firm supervising one or more of the firm's accounting or auditing engagements or carrying out a quality control function on the firm's accounting or auditing 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* (previously referred to as an unmodified report) on its most recently accepted System or

Engagement Review that was accepted timely, ordinarily within the last 3 years and 6 months[8] (see Interpretation No. 31b-1).

c. demonstrate proficiency in the standards, interpretations, and guidance of the program (see Interpretation No. 33-1).

A majority of the report acceptance body members and the chairperson charged with the responsibility for acceptance of System Reviews should possess the qualifications required of a System Review team captain.

A national list of consultants will be maintained by the AICPA, so that the administering entity has an available pool of consultants with GAS, ERISA, FDICIA, ~~and~~ carrying broker-dealer, and service organization experience to call upon in the instance when it does not have an experienced RAB member to consider the review of a firm when circumstances warrant. The national RAB consultant would not necessarily have to participate physically in the RAB meeting (teleconference option). The national RAB consultant will not be eligible to vote on the acceptance of a review. Determination that a review requires a national RAB consultant should be made prior to assigning the review to a RAB. The national RAB consultant would have to meet the following qualifications for RAB participation:

a. Currently active in public practice at a supervisory level in the accounting or auditing function of a firm enrolled in the program, as a partner of the firm, or as a manager or person with equivalent supervisory responsibilities. To be considered currently active, a consultant should be presently involved in the supervision of one or more of his or her firm's accounting or auditing engagements or carrying out a quality control function on the firm's accounting or auditing engagements. To be considered a consultant on GAS, ERISA, FDICIA, ~~or~~ carrying broker-dealer, or service organization engagements, the current activity must include the respective industry asked to consult upon.

b. 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" (previously referred to as an unmodified report) on its most recently accepted System Review that was accepted timely, ordinarily within the last three years and six months.

c. Not associated with an engagement that was deemed not performed in accordance with professional standards on the consultant's firm's most recently accepted System Review.

A report acceptance body member who is suspended or restricted from scheduling or performing peer reviews no longer meets the qualifications until such suspension or restriction is removed. Reinstatement as a report acceptance body member would be at the discretion of the administering entity or committee.

[8] If a committee member firm's most recent review was a report review, then the member is not eligible to be charged with the responsibility for acceptance of any peer reviews.

Technical Reviewers

Each technical reviewer charged with the responsibility for performing technical reviews should

a. demonstrate proficiency in the standards, interpretations, and guidance of the program applicable to the type of peer reviews being evaluated and that meet the requirements of the team captain or review captain training requirements established by the board (see Interpretation No. 33-1).

b. participate in at least one peer review each year, which may include participation in an on-site oversight of a System Review.

c. have an appropriate level of accounting and auditing knowledge and experience suitable for the work performed. Such knowledge may be obtained from on-the-job training, training courses, or a combination of both. Technical reviewers are to obtain a minimum amount of CPE to maintain the appropriate level of accounting and auditing knowledge.

   If a technical reviewer does not have such knowledge and experience, the technical reviewer may be called upon to justify why he or she should be permitted to perform technical reviews or oversights. The administering entity has the authority to decide whether a technical reviewer's knowledge and experience is sufficient and whether he or she has the capability to perform a particular technical review or oversight whether there are high-risk engagements involved or other factors.

   The fundamental purpose of CPE is to maintain or increase, or both, professional competence. AICPA members are required to participate in 120 hours of CPE every 3 years. In order to maintain current knowledge of accounting, auditing, and quality control standards, technical reviewers should obtain at least 40 percent of the AICPA-required CPE in subjects relating to accounting, auditing, and quality control. Technical reviewers should obtain at least 8 hours in any 1 year and 48 hours every 3 years in subjects relating to accounting, auditing, and quality control. The terms *accounting, auditing,* and *quality control* should be interpreted as CPE that would maintain current knowledge of accounting, auditing, and quality control standards for engagements that fall within the scope of peer review as described in paragraphs .06–.07 of the standards.

   Technical reviewers have the responsibility of documenting their compliance with the CPE requirement. They should maintain detailed records of CPE completed in the event they are requested to verify their compliance. The reporting period will be the same as that maintained for the AICPA.

   A technical reviewer who is also a peer reviewer and is suspended or restricted from scheduling or performing peer reviews no longer meets the qualifications until such suspension or restriction is removed. Reinstatement as a technical reviewer would be at the discretion of the administering entity or committee.

Exhibit A

Service Organization Control Engagements: Background and Other Information Considered

SOC 1 Engagements

A service organization control (SOC) 1 report is a report on controls at a service organization relevant to user entities' internal control over financial reporting. Under SOC 1, which is synonymous with SSAE 16 and AT 801, *Reporting on Controls at a Service Organization*, a service organization provides a very detailed description of its controls that are relevant to user entities' internal control over financial reporting. The service auditor reports on whether the description is fairly presented, whether the controls are suitably designed, and in a Type 2 SOC 1 engagement, whether the controls were operating effectively. These engagements were previously performed under SAS 70, Service Organizations. Like SAS 70, SOC 1 is a restricted-use report, intended for use by user entities of the service organization and their financial statement auditors. A practitioner may perform either a Type 1 or Type 2 SOC 1 engagement. SOC 1 reports are intended to meet the needs of management of user entities and their user auditors. A SOC 1 report provides information to user auditors to assist them in determining the nature, timing, and extent of the audit procedures to be performed and whether they may rely on controls implemented by the service organization.

SOC 2 & 3 Engagements

Consistent with SAS 70, SOC 1 engagements should not be used for reporting on controls over subject matter other than financial reporting. The AICPA has introduced two new reports to meet the needs of user entity management and the general public for assurance over non-financial reporting related controls. SOC 2 and SOC 3 engagements are performed under AT 101, *Attest Engagements*. SOC 2 engagements are also performed under the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.* SOC 2 engagements require an examination and SOC 3 engagements may be an examination, review, or agreed upon procedure.

SOC 2 Engagements

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 a SOC 1, SOC 2 provides for both Type 1 and Type 2 reports.

Unlike SOC 1, the primary users of SOC 2 reports generally are not user auditors but rather management of the user entities to make operational decisions. For example, a user entity may make certain commitments to its customers regarding the security of the system it uses to process customers' information. When such processing is outsourced to a service organization, the user entity's ability to meet these commitments may, in large part, depend on controls at the service organization that affect physical and logical access to the system. For example, an increasingly popular service offered by certain service organizations is cloud computing, which involves providing user entities with on-demand network access to a shared pool of computing resources, such as networks, servers, storage, applications, and services. The increasing use of these services has resulted in a demand by user entities for assurance regarding controls over the systems underlying those services.

Many user entities are required by law or regulation to maintain the privacy of the information they collect from customers, including the privacy of that information when it is at a service organization. For example, a service organization that digitizes health records for users has full access to health records that contain very sensitive information. Organizations subject to the Health Insurance Portability and Accountability Act (HIPAA) requirements can demonstrate their compliance with their privacy commitments through a SOC 2 report that addresses the privacy principle. Another example of a situation in which a SOC 2 report would be useful is a service organization that provides document management services to user entities. Such services may include scanning hard copies of legal files, indexing the data, and storing the data for user entities. In addition to concerns about maintaining the privacy of such data, user entities would also be concerned about the possibility of errors or omissions in the data resulting from system problems that might occur during scanning, indexing, and storing the data. A SOC 2 report that addresses the privacy principle and the processing integrity principle would be useful in this situation. In the case of a data center that hosts numerous companies' IT environments, the risk of continuity of processing and internet connectivity and environmental safeguards to restrict access and protect the equipment would entice a user entity to obtain a SOC 2 addressing the availability principle. The criteria for these engagements are the criteria in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*).

SOC 3 Engagements

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. In the illustrative SOC 3 examination report included in TSP section 100, the practitioner expresses an opinion on whether the service organization maintained effective controls over its system, based on the applicable trust services criteria. Although a SOC 3 report is designed to meet the needs of a broad range of users, it does not contain a detailed description of the service auditor's tests of the operating effectiveness of controls and the results of those tests, which may be necessary for a particular user to determine how it is affected by those controls.

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 are general-use reports, which means they may be used by anyone and therefore can be used by the service organization to market its services to potential customers. Management of a service organization may consider engaging a service auditor to perform a SOC 2 engagement and a SOC 3 engagement and to report on both engagements. A SOC 3 report that addresses the

privacy principle will also cover the service organization's compliance with the commitments in its statement of privacy practices.

Alternative to Must Select
The Board considered making examinations of service organizations (SOC 1 and 2) must cover engagements as an alternative to must select engagements. Must select industries must be included in the sample of engagements selected for review. A must cover industry does not have to be selected for review; however, either the team captain or a team member must have at least recent experience (within last 5 years) in the industry (resume codes A, B, or C) to aid in the risk assessment process and determination of whether an engagement from the must cover industry should be selected for review. There are no must cover industries for Engagement Reviews. Peer review staff periodically assesses industries to determine which may have the most significant public interest of the moment. Currently, the list includes HUD, school districts, and state and local government. These industries, in addition to the current must select industries (as described in Interpretation 63-1), are must cover industries for all firms. An individual firm may have additional must cover industries based on the concentration of its accounting and auditing (A&A) practice. Industries in which a firm's A&A practice has a 10% or more concentration or the firm's three largest industry concentrations (if none represent more than 10%), are also considered must cover industries. All must select industries are must cover industries, however, all must cover industries are not must select industries.

Further, the Board recently approved a revision to Interpretation 59-1. Interpretation 59-1 explains that a reasonable cross section of a firm's A&A practice not only includes consideration of the specific industries that are required to be selected, but also other industries with a significant public interest. The interpretation also now defines industries that have a significant public interest as those that benefit the general welfare of the public, such as those that have recent regulatory and legislative developments (for example, broker-dealers). Public interest industries will vary across firms and reviewers should consider the composition of a firm's A&A practice when determining if their risk assessment should address a public interest industry. As a must cover industry, team captains would be required to document specific considerations made in regards to making the decision of whether to select and how many to select, such as the types of SOCs (1, 2, or 3), experience of partners with the type of engagement, and CPE/knowledge of SOCs, reasonability of fees charged for SOC service.

Team Member Experience and Report Acceptance Bodies (RAB)
As with other must select engagements, either the team captain or a team member must have at least recent experience in the practice area or industry (resume codes A, B, or C) to aid in the risk assessment process and determination of which engagements and how many should be selected. Reviews for firms that perform SOC 1 engagements will require a team member with SOC 1 experience. Reviews for firms that perform SOC 2 engagements will require a team member with SOC 2 experience. A team member with attestation experience is sufficient for reviews of firms that perform SOC 3 engagements.

Further, a member of the RAB should also have SOC 1 and/or SOC 2 experience, respectively to consider the review of a firm that performs those engagements. An approved consultant may be used by the RAB when necessary. A national list of consultants will be maintained by the AICPA, so that the administering entity has an available pool of consultants with SOC 1 and SOC 2 experience to call upon in the instance when it does not have an experienced RAB member to consider the review of a firm when circumstances warrant. See Interpretation 132-1 for the qualifications of a national RAB consultant.

Conclusion

The Board considered the information above, including the alternative approach to having SOCs as must select engagements, and has determined that having both SOC 1 and SOC 2 engagements as must selects will assist the Board to accomplish its goal of improving the quality of services provided by AICPA members and protect the interests of the general public. The Board believes that addressing SOC 3 engagements in the peer reviewer's risk assessment is adequate.

As we move forward with the new SOC engagements, the subject matter is more complicated, the business models are more complicated, and the inherent risk scenarios represented by what accountants are reporting on is significant. The number of these types of engagements performed is going to become much more voluminous than in the past due to the ability to provide SOC 2 and SOC 3 engagements.

Even though user auditors will not rely on SOC 2 reports like SOC 1 engagements, there is an incredible array of services that are being performed on an outsource basis that represent inherent risk to the users and perspective users. As the nature of these services is changing (as entering a cloud based dominated world) and with the increased use of technology, companies outsource functions to subject matter experts. Reliance upon service organizations for these important business functions are not internal control over financial reporting relevant but reflect a critical business decision. A CPA may perform a SOC 1 engagement; however, a SOC 2 engagement would generally be performed by a CPA with an IT background or by a CPA using the work of an IT specialist.

Service organizations provide services that affect many user entities. The concept underlying a SOC 1 or SSAE 16 engagement is that the service auditor stands in the shoes of all the user auditors and performs procedures that the user auditor would have performed if (1) the service organization permitted throngs of user auditors to visit the service organization and perform procedures there and (2) the user auditors had the IT expertise and other specialized knowledge frequently required to perform these engagements. The same can be said for the service auditor performing a SOC 2 engagement who stands in the shoes of management of the user entities and performs procedures that provide information and assurance to the user entities about the security, availability, or processing integrity of the service organization's system, or the confidentiality or privacy of the information processed by the system.

The Board believes it should do everything it can to promote and ensure the integrity of services related to SOC reporting because of the large number of user auditors and user entities that use such reports.