THOMSON REUTERS
CHECKPOINT™

S. Davis & Associates, P.A.
Certified Public Accountants & Consultants

THE PPC
ACCOUNTING AND AUDITING UPDATE

JUNE 2021, VOLUME 30, NO. 6

AICPA Issues Guidance on Performing Third-party Assessment Engagements

The AICPA issued new non-authoritative guidance in January 2021 for CPA firms that perform third-party assessment engagements. These engagements constitute professional services. Technical Questions and Answers (TQAs) 9550.01 and 9550.02 provide the program requirements and the steps for CPAs to follow to comply with current professional standards, including the *AICPA Code of Professional Conduct*, and they clarify when a member is required to perform the engagement in accordance with the AICPA Statements on Standards for Attestation Engagements (SSAEs).

What Is a Third-party Assessment Program?

A "program body" (federal or state government agency, industry consortium, or group of subject matter experts) may develop a third-party assessment program to obtain information about a specific subject from its members or third parties it does business with, including vendors, contractors, or customers. The program body uses a third-party assessor to provide and evaluate the information based on its requirements or instructions so it can determine whether to provide an approval, certification, or authorization. Both CPAs and non-CPAs can be assessors.

A third-party assessment program includes all the following characteristics:

- a publicly available framework with criteria for a third party to use to evaluate the subject matter;
- evaluation of the subject matter against the program's framework (and a self-assessment by the entity);
- approval of the assessor (individual or organization) based on experience or educational requirements, and there may be guidelines for evaluating the assessor's work quality and objectivity or independence;
- requirement that the assessor must comply with the requirements and instructions in the program, including the procedures to perform and how to communicate the results and conclusions to the program body.

In this Issue:

This newsletter is also available online.
Please call (800) 431-9025, or order online:
https://tax.thomsonreuters.com/products/brands/checkpoint/ppc/

THOMSON REUTERS™

Which Professional Standards are Required to Be Applied to the Engagement?

The AICPA Code's *General Standards Rule* (ET sec. 1.300.001) requires professional competence, due professional care in performing the services, adequate planning and supervision, and obtaining sufficient relevant data as a basis for any conclusions or recommendations.

Independence requirements must be applied, including the assessment program's defined requirements and the AICPA Code's *Independence Rule* (ET sec. 1.200.001) if the assessment is performed as an attest engagement. If it isn't an attest engagement but the member performs another engagement for the entity that requires independence, the *Nonattest Services* subtopic's (ET sec. 1.295) independence safeguards must be applied.

If an examination, review, or agreed-upon procedures report is issued for the third-party assessment, the engagement must be performed in accordance with the SSAEs. Statements on Standards for Consulting Services may be applied. Reports issued other than those under the SSAEs must be clearly distinguishable from reports issued under the SSAEs.

Practical Consideration:

The complete text of the TQAs is available on the AICPA's website at **www.aicpa.org/content/dam/aicpa/interestareas/frc/downloadabledocuments/tqa-sections/tqa-section-9550-01-02.pdf**.

• • •

FASB Clarifies Accounting for Callable Debt Securities

The FASB issued ASU 2020-08, *Codification Improvements to Subtopic 310-20, Receivables—Nonrefundable Fees and Other Costs*, to simplify the accounting for callable debt securities. The amendments in this Update clarify guidance in ASU 2017-08, *Receivables—Nonrefundable Fees and Other Costs (Subtopic 310-20): Premium Amortization on Purchased Callable Debt Securities*, which required premiums on callable debt securities to be amortized to the earliest call date. This ASU clarifies that an entity should reevaluate whether a callable debt security with multiple call dates is within the scope of FASB ASC 310-20-35-33 for each reporting period. This ASU doesn't change the effective dates of ASU 2017-08.

For public business entities, the amendments are effective for fiscal years, and interim periods within those fiscal years, beginning after December 15, 2020. Early application isn't permitted. For all other entities, the amendments are effective for fiscal years beginning after December 15, 2021, and interim periods within fiscal years beginning after December 15, 2022. Early application is permitted for all other entities for fiscal years, and interim periods within those fiscal years, beginning after December 15, 2020. All entities should apply the amendments prospectively as of the beginning of the period of adoption for existing or newly purchased callable debt securities.

• • •

FASB Issues Codification Improvements

In October 2020, the FASB issued ASU 2020-10, *Codification Improvements*. The FASB has a standing project on its agenda to make improvements and clarifications to GAAP and to address suggestions it receives from stakeholders to clarify or simplify the standards. This ASU provides clarification on a variety of topics and is intended to improve consistency of disclosures by adding the existing disclosure requirements to the relevant disclosure sections of the Codification.

The amendments in this ASU don't change GAAP but are intended to address inconsistent application of the guidance in practice, which could result in some entities changing their current financial reporting. The codification improvements apply to all reporting entities that are within the scope of the accounting guidance affected by the amendments.

Continued on page 5

The PPC Technology Update

by Roman H. Kepczyk, CPA.CITP, CGMA

What to Do if Your Firm Is Hacked

Accounting firms are being targeted by cybercriminals for the significant amount of PII (personally identifiable information) and financial data which the firms have been entrusted with by their clients. The size of firm doesn't matter to the hacker groups. While larger firms may provide a bigger payday, medium and smaller firms are often easier targets and at higher risk, as they often don't have the security defenses, cyber training, or technical resources to protect their firm from being hacked. All it takes is one employee inadvertently clicking on a compromised link in a phishing email or text message, plugging in an infected USB thumb drive, re-using a compromised password, or not updating their computer or WiFi router timely, and the hackers are on their way to taking control of the firm's computer systems and data. When that happens, your firm better be prepared.

Firms will benefit from having a written incident response plan which they have walked through previously with firm owners, as the worst time to plan a breach response is after it has occurred. The focus of the plan should be on minimizing damage and providing a measured, thoughtful response that shows the firm has taken back control. To help firms get started, below we outline the key components of breach incident response, as well as considerations in communicating the breach to employees, clients, and other vested parties.

Incident Response Team

The incident response team should include firm owners, IT personnel, key vendors, and cyber security resources. This includes external security expertise with forensic skills to identify and remediate the breach, law enforcement contacts and legal resources to ensure the firm responds appropriately to regulatory requirements, and the skills of a public relations firm may be required to communicate the plan. If the firm has cybersecurity insurance, the provider may already have many of these resources available to the firm. The firm should work with the provider to document these contacts.

Incident Response Plan

The incident response plan should be written in a concise step by step format which is readily available to key stakeholders (i.e., a PDF on their smartphone or hardcopy in the firm manager's office). While prevention should be one of the primary responsibilities of the firm's IT security team, policies must be in place to detect a possible breach and to notify the security team of anomalies so they can be investigated. This includes educating employees on "warning signs" that they may have been hacked. If the IT team identifies that a potential breach incident has occurred, they will invoke procedures to stop the intrusion and contain the damage as much as possible. This will most likely require the assistance of external cybersecurity and forensic expertise, who will have the depth of experience in eradicating various threats and solutions necessary to prevent a recurrence. This is particularly important if the firm's files are encrypted with ransomware requiring backups to be restored that may also be infected with malware. The firm should work with attorneys that understand the regulatory and reporting requirements (such as public notification, credit reporting, etc.), as well as the local FBI office, before communicating the incident. As cyber threats continue to evolve, it is important for the firm to review, update, and walk through their incident response plan at least annually.

Incident Communications

The final phase of the incident response plan is communicating the breach information publicly, which should be done in a coordinated, measured way so it is obvious that the firm has taken control of the situation. Consider the following when creating your response plan.

- **Timely Response.** One of the first questions that firm owners will need to respond to is "When did you first become aware of the breach?" Studies have shown that the quicker and more thoroughly a firm responds to a cyber breach, the smaller the financial consequences. Consequently, it is imperative that the firm have an incident response plan and team in place to respond quickly to a breach.
- **Transparency.** Being truthful and accurate in communicating breach information is important to sustain trust with employees and clients throughout the breach event. After the cause and extent of the breach have been identified, and the firm has implemented a plan to remediate the damage (including steps to ensure that it will not happen again), these steps should be laid out in a comprehensive factual manner. The message should also include the legal and regulatory requirements for impacted clients and renumeration that the firm will provide to those that have been impacted.
- **Controlled Message.** Controlling the message to provide a consistent response is critical as incomplete or conflicting information creates speculation and uncertainty. The incident response plan should identify a central representative who will deliver the message to firm personnel, clients, and the media, if necessary, so they are all getting the same information as close to the same timeline as possible.
- **Confident Remediation.** One of the most important components of incident communication is outlining the steps the firm has taken to remediate the breach. This would include the response and solutions the firm has implemented, as well as the training of firm personnel to minimize the possibility that this type of breach could occur again. The firm must also be able to lay out how they are meeting the regulatory requirements of notification and assisting clients and other impacted parties potentially impacted by the breach.

While no one wants to be hacked, the reality is that it is more likely a matter of "when" rather than "if" the firm will experience a cyber event. Having a qualified team in place, either independently identified or organized through your cyber insurance carrier, will ensure you can respond quickly. And finally, being prepared for such an event with a written incident response plan will minimize the financial and reputational damage the firm will experience.

Roman H. Kepczyk, CPA.CITP, CGMA is Director of Firm Technology Strategy for Right Networks and partners exclusively with accounting firms on production automation, application optimization, and practice transformation. He has been consistently listed as one of INSIDE Public Accounting's Most Recommended Consultants, Accounting Today's Top 100 Most Influential People, and CPA Practice Advisor's Top Thought Leader to the accounting profession.

Continued from page 2

The amendments are in two Sections:

Section B

Section B contains amendments that improve the consistency of the codification by including all disclosure guidance in the Disclosure Section, Section 50, of the Codification. Previously, certain disclosures were included elsewhere in the ASC, particularly in Section 45, Other Presentation Matters, when presentation could be made either on the face of a financial statement or within the notes. This change is intended to make it less likely that preparers will miss the disclosure requirements.

Some of the disclosure areas included in this Section are:

- income taxes and reclassification adjustments in reporting comprehensive income and accumulated other comprehensive income (FASB ASC 220-10)
- accounting changes and error corrections (FASB ASC 250-10)
- earnings per share (FASB ASC 260-10)
- notes payable with imputed interest (FASB ASC 835-30)

Section C

Section C includes guidance intended to make application of the standards clearer in a number of areas, including interim reporting (FASB ASC 270-10), transfers of financial assets including receivables (FASB ASC 310-10), foreign currency matters (FASB ASC 830), and updates to the Master Glossary. The FASB also added cross references to other guidance, headings, and refinements to make certain standards clearer.

Effective Date

The amendments are effective for annual periods beginning after December 15, 2021, and interim periods within annual periods beginning after December 15, 2022, with early application permitted for any annual or interim period for which financial statements are available to be issued. The guidance is effective one year earlier for public entities, with early application permitted for any annual or interim period for which financial statements haven't been issued. The amendments should be applied retrospectively, at the beginning of the period that includes the adoption date.

Practical Consideration:

The ASU is available on the FASB's website at **www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1176175510147&acceptedDisclaimer=true**.

• • •

FASB Provides a Practical Expedient for Private Company Franchisors

In January 2021, the FASB issued ASU 2021-02, *Franchisors—Revenue from Contracts with Customers (Subtopic 952-606): Practical Expedient*, intended to reduce the cost and complexity of applying FASB ASC 606. The amendments in this Update provide a new practical expedient for certain franchisors to simplify the identification of performance obligations in Step 2 of the revenue recognition guidance. They apply to franchisors that aren't public business entities within the scope of Topic 952.

Under guidance in FASB ASC 606, preopening services provided to franchisees in franchise agreements must be analyzed by the franchisor to determine whether they represent promised goods or services, are distinct from the franchise license and from each other, and should be accounted for as separate performance obligations. Preopening services provided to franchisees include activities such as training personnel, assisting in site selection, obtaining and preparing facilities for use, setting up recordkeeping and IT, and other advice provided by the franchisor.

The practical expedient is intended to reduce the existing cost and complexity of identifying performance obligations related to pre-opening services in franchise agreements. The amendments don't change other guidance in FASB ASC 606.

Pre-opening services provided to a franchisee may be accounted for as distinct from the franchise license if

The PPC Accounting and Auditing Update is published monthly by Thomson Reuters/Tax & Accounting, P.O. Box 115008, Carrollton, Texas 75011-5008, (800) 431-9025.

THOMSON REUTERS™

Tax & Accounting - Checkpoint
P.O. Box 115008
Carrollton, Texas 75011-5008
UNITED STATES OF AMERICA

ADDRESS SERVICE REQUESTED

PRSRT STD
U.S. POSTAGE
PAID
Thomson

the services are consistent with the predefined services listed in the ASU. If the promised goods and services aren't consistent with those in the list, or if the entity doesn't elect the practical expedient, guidance in FASB ASC 606 on identifying performance obligations must be applied. This determination affects the timing of the revenue recognition of initial franchise fees.

In addition, franchisors that elect to use the practical expedient can make an accounting policy election to account for all qualifying pre-opening services as a single performance obligation.

For the most part, ASU 2021-02 is effective immediately. If an entity already adopted FASB ASC 606, the amendments are effective in interim and annual periods beginning after December 15, 2020, and should be applied retrospectively to the date FASB ASC 606 was adopted with a cumulative effect adjustment recorded to retained earnings. Early application is permitted.

If an entity hasn't adopted FASB ASC 606, the transition provisions and effective date in paragraph 606-10-65-1 apply, which allows for either modified retrospective or full retrospective transition, and the effective date is for fiscal years beginning after December 15, 2019, and interim periods within fiscal years beginning after December 15, 2020. Entities electing the practical expedient must disclose the accounting policy election, and the guidance in this ASU should be applied consistently to contracts in similar circumstances and with similar characteristics.