THOMSON REUTERS
CHECKPOINT™

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

THE PPC
ACCOUNTING AND AUDITING UPDATE

NOVEMBER 2019, VOLUME 28, NO. 11

PCAOB Adopts New Standard on Estimates

On December 20, 2018, the PCAOB issued Release 2018-005, *Auditing Accounting Estimates, Including Fair Value Measurements, and Amendments to PCAOB Auditing Standards*. The revised standard and related amendments, which were approved by the SEC on July 1, 2019, will be effective for audits of financial statements for fiscal years ending on or after December 15, 2020.

Objectives

The new auditing standard and related amendments on auditing estimates and fair value are designed to create a more risk-based approach to this complex, judgment-based area that is of increasing importance to investors. As a number of significant new accounting standards become effective, estimates become more prevalent in financial statement items and disclosures. Valuations, impairments, expected credit losses, and revenues from contracts with customers all involve significant estimates by management. Due to their complexity, uncertainty, and susceptibility to fraud or bias, estimates generally present greater risk than other audit areas, requiring special attention from auditors in response.

Background

In August 2014, the PCAOB issued a staff consultation paper on auditing estimates and fair value measurements that addressed a broad range of topics. After analysis of the comments received, as well as feedback from the PCAOB's Standing Advisory Group (SAG) and the Investor Advisory Group (IAG) meetings and other monitoring and outreach activities, including monitoring the IAASB's current project on accounting estimates, the PCAOB developed a proposed standard in June 2017 (Release No. 2017-002). The final new standard builds on current auditing techniques and practices, but with increased emphasis on audit risk and professional skepticism. In addition, the Board considered advances in technology and crafted the standard to be flexible for the use of new tools by auditors and companies.

In this Issue:

Key Provisions

Some key provisions of the new standard include—

- Enhancing and clarifying requirements to consider and address potential management bias.
- Creating a more consistent substantive testing approach by extending some requirements from current standards on auditing fair value measurements to all accounting estimates in significant accounts and disclosures.
- Further integrating requirements with the risk assessment standards, emphasizing greater focus on estimates with higher risk of material misstatement.
- Providing additional clarity and specificity on procedures for auditing accounting estimates.
- Adding requirements that specifically apply to auditing the fair value of financial instruments, such as the use of information from pricing services, broker-dealers, and other pricing sources.

The new standard replaces and renames AS 2501, *Auditing Accounting Estimates*, as AS 2501 (Revised), *Auditing Accounting Estimates, Including Fair Value Measurements*. It also rescinds AS 2502, *Auditing Fair Value Measurements and Disclosures*; AS 2503, *Auditing Derivative Instruments, Hedging Activities, and Investments in Securities;* and AI 16, *Auditing Accounting Estimates: Auditing Interpretations of AS 2501*. In addition, it amends the following:

- AS 1015, *Due Professional Care in the Performance of Work*.
- AS 1105, *Audit Evidence*.
- AS 1205, *Part of the Audit Performed by Other Independent Auditors*.
- AS 2110, *Identifying and Assessing Risks of Material Misstatement*.
- AS 2301, *The Auditor's Responses to the Risks of Material Misstatement*.
- AS 2401, *Consideration of Fraud in a Financial Statement Audit*.
- AS 2805, *Management Representations*.
- Other conforming amendments.

Practical Consideration:

The full text of Release 2018-005 is available at **https://pcaobus.org/Rulemaking/Docket043/2018-005-estimates-final-rule.pdf**.

New EBP SAS

In July 2019, the AICPA Auditing Standards Board (ASB) issued SAS 136, *Forming an Opinion and Reporting on Financial Statements of Employee Benefit Plans Subject to ERISA*.

SAS 136 creates new reporting requirements and performance requirements unique to auditing ERISA plans. The new SAS will cause significant changes to the form and content of the auditor's report on plan financial statements as well as ERISA-required supplemental schedules.

Highlights

Highlights of SAS 136 include—

- *No More "Limited Scope" Audits.* Audits performed pursuant to ERISA section 103(a)(3)(C) will no longer be referred to as "limited scope audits," but will now be referred to as "ERISA section 103(a)(3)(C) audits." The new audit standard includes new performance and reporting requirements specific to ERISA section 103(a)(3)(C) audits.
- *Report on Audited Financial Statements.* The content of the standard aligns with the requirement of SAS 134, *Auditor Reporting and Amendments, Including Amendments Addressing Disclosures in the Audit of Financial Statements*.
- *Management Responsibility.* SAS 136 provides clarity on management's responsibilities during the audit. New engagement acceptance requirements state that the auditor will request plan management to acknowledge in the engagement letter management's responsibilities, including the following:
  - Maintaining a current plan instrument, including all plan amendments.
  - Administering the plan and determining that any of the transactions presented and disclosed in the plan financial statements are in conformity with the plan's provisions, including sufficient records for plan participants.
  - Providing a draft Form 5500 prior to the dating of the auditor's report.
  - When management elects to have an ERISA Section 103(a)(3)(C) audit, determining whether—
    - Investment information is prepared and certified by a qualified institution, as described in 29 CFR 2520.103-8,
    - The certification meets the requirements in 29 CFR 2520.103-5, and

Continued on page 5

The PPC Technology Update

by Roman H. Kepczyk, CPA.CITP, CGMA

Mobile Security Awareness

October has been designated National Cybersecurity Awareness Month, and, with that in mind, we have created a listing of mobile security considerations that every auditor should understand and adhere to. Every team member should be held accountable for following firm policies and procedures designed to protect the firm's equipment and secure client information. Below, we outline eight critical areas of concern:

- **Secure Operating System.** One of the first steps in securing mobile devices should be to ensure that the most current operating system is running and that system updates are being implemented. The majority of accountants use Microsoft Windows and should plan on updating all workstations to Windows 10 before Microsoft discontinues technical support for Windows 7 on January 14, 2020. Windows updates should be set to update automatically or under the direction of the firm's IT personnel and all personnel should be directed to reboot their computers daily so these new updates will be installed timely.
- **Secure Access.** In addition to using complex passwords or passphrases to log in to the computer and the firm's network, firms should mandate the use of multi-factor authentication tools or password wallets to minimize the impact of a hacker obtaining an auditor's login credentials and posing as the auditor. Firm policies should also require users to lock their Windows screen or logout entirely when they leave their workstation. In addition, the user's screen should be set to automatically lock after a specified period of time (usually less than 20 minutes).
- **Secure Applications.** Along with operating system updates, firms should mandate that antivirus and malware applications be updated regularly on any computer and any mobile device connecting to the firm's information resources. All local programs, such as Microsoft Office, engagement binders or accounting and assurance applications should be updated regularly under the IT department's direction or managed entirely in a cloud environment such that the auditor gets the most updated version each time they log in.

- **Secure Connection.** Auditors should primarily use the mobile hotspot within their cellphone or a shared MiFi/Jetpack mobile hotspot to connect to the firm's data resources when working remotely, in lieu of checking out work to their local workstation and/or connecting to a client or public WiFi system. If auditors use a client's Internet connection for remote access, the auditor should use a virtual private network (VPN) implemented by the firm's IT personnel to encrypt the connection. It is recommended that public WiFi *not* be utilized to connect any firm workstation to the Internet. If any data is stored on the auditor's local hard drive, full disk encryption should be mandatory to protect the data in the event the workstation is lost or stolen. Preferably all data and applications should only run in the cloud to ensure no client data is at risk of physical theft. Firmware on the auditor's mobile hotspot and any router should also be updated regularly to protect those devices.
- **Physical Security.** Often overlooked in training, firms should remind personnel that their workstation should be locked up when unattended either in a secure location or via a cable lock. (There are dual locks to also secure the use of an external monitor.) Physical security also extends to laptops in transit and should include tips such as always physically touching the computer bag/strap when not using it or placing it in the trunk or hiding it in the backseat when *leaving* the office or a client location rather than when arriving at the next location, where an unscrupulous observer might tip off a thief. The use of USB flash drives should

also be disallowed, as they pose a security risk if lost or misplaced as well as a malware threat if a client provides their data on an infected device. Auditors should train clients on using digital portals and secure email instead.

- **Mobile Devices.** Firms that allow the use of personal smartphones, tablets, and home computers to access firm resources should also update their security policies for these devices accordingly. This includes requiring a secure passcode/fingerprint to access any such devices, tools such as mobile device management to ensure that only pre-authorized devices can access the firm's information systems from them, and the ability to remotely erase the firm's data from the device in the event of loss or theft. This should also be included in the firm's IT policies.
- **Policies and Governance.** The firm's IT team (and external security resource if used) should meet with Human Resources annually to review and update policies to take into account technological evolution and incorporate firm policy changes such as moving to the cloud, social networking, remote and flextime workers, and disallowance of USB flash drives prior to doing any annual HR/Security training.
- **Security Training.** Audit and remote staff should not be excluded from mandatory security training, which is recommended for all firm personnel on at least an annual basis. In addition, the firm should provide ongoing reminders on current phishing campaigns during key scamming periods (holidays, year ends, and tax deadlines). Training should be done in conjunction with the firm's external security provider and should include secure computing practices (i.e. looking for the padlock and https: in browser addresses to verify a secure remote connection). Training should also include warning signs if the user suspects their computer has been breached and instructions on how to respond (i.e. not turning off the computer but instead disconnecting from the Internet by turning off the WiFi or pulling out the Ethernet cable and then notifying the IT department).

Security of firm resources and client information is everyone's responsibility, especially when working remotely. Accounting profession best practices point to the firm's IT, Human Resources, and external security group working together with remote staff to educate and understand the firm's policies and security procedures.

Roman H. Kepczyk is the Director of Firm Technology Strategy for Right Networks and consults exclusively with accounting firms throughout North America to transform them towards today's digital best practices and technologies. In addition to being a CPA.CITP, he is a Lean Six Sigma Black Belt and incorporates Lean Six Sigma methodologies to help firm's optimize their production workflows.

Continued from page 2

  - The certified investment information is appropriately measured, presented, and disclosed in accordance with the applicable financial reporting framework.

- *Risk Assessment and Responses.* The auditor should obtain and read the most current plan instrument as part of obtaining an understanding of the entity sufficient to perform risk assessment procedures. The auditor should also consider relevant plan provisions that affect the risk of material misstatement when designing and performing audit procedures.
- *Management Representations.* The new standard requires that the auditor obtain written management representations at the conclusion of the engagement regarding their plan responsibilities. It also includes a new acknowledgement related to management's responsibility with respect to the investment certification when management elects to have an ERISA Section 103(a)(3)(C) audit.
- *Communication with Management and Those Charged With Governance.* SAS 136 requires the auditor to communicate with management and/or those charged with governance, as follows:
  - Reportable findings must be communicated in writing to management and those charged with governance in a timely manner.
  - The auditor must discuss with management any prohibited transactions that haven't been properly reported in the supplemental schedule required by ERISA.
  - The auditor must communicate to those charged with governance the auditor's responsibility regarding the Form 5500 procedures performed and the results of such procedures.
- *Form 5500.* The new SAS requires management to provide the auditor with a draft of Form 5500 so that the auditor may review the draft for material inconsistencies with audited ERISA plan financial statements in order to determine if either the draft or the financial statements require revision.

Effective Date

SAS 136 is effective for audits of ERISA plan financial statements for periods ending on or after December 15, 2020. Early implementation isn't permitted. The SAS applies only to audits of employee benefit plans that are subject to ERISA.

Practical Consideration:

The EBP SAS is available at **www.aicpa.org** and on Checkpoint at **https://checkpoint.riag.com**.

AICPA Technical Q&A Activity

The AICPA recently deleted two attestation Q&A sections, Q&A 9520, *Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization*, and Q&A 9530, *Service Organization Controls Reports;* and revised Q&A 6140, *Not-For-Profit Entities.*

In addition, the AICPA recently issued new Technical Question and Answers (Q&A) 9110.24–.27 relating to the OMB 2019 Compliance Supplement. Following is a brief discussion of the new Q&A:

- **9110.24, Background to Sections 9110.25–.27—OMB 2019 *Compliance Supplement*.** The OMB 2019 Compliance Supplement revised the approach used to identify the compliance requirements subject to the compliance audit. Each federal agency was mandated by OMB to limit the number of compliance requirements subject to the audit to six, with the exception of the Research and Development cluster, which was permitted to identify seven compliance requirements as subject to the audit. The auditor will still have to determine whether the requirements could have a direct and material effect on the program.
- **9110.25, Opining on Compliance When the OMB *Compliance Supplement* Excludes Direct and Material Compliance Requirements From the Scope of a Single Audit.** 9110.25 addresses whether an auditor can provide an opinion on compliance if the supplement excludes certain types of compliance requirements from the scope of the audit and the auditor is aware that one or more of those excluded requirements could have a direct and material effect on a major federal program. AU-C 935 indicates that the auditor should form an opinion at the level

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

specified by the governmental audit requirement. In this case, the governmental audit requirement is the supplement, which specifies the compliance requirements to be considered by the auditor. Therefore, the auditor can provide an opinion on compliance.

- **9110.26, Effect on Auditor Reporting Due to the OMB *Compliance Supplement* Change in Approach for Identifying the Requirements Subject to the Single Audit.** 9110.26 addresses whether the auditor is required to revise the report wording for the report on compliance for each major federal program. AU-C 935 indicates that the auditor should include the identification of the applicable compliance requirements or a reference to where they can be found in the introductory paragraph of the report.
- **9110.27, Including an Other-Matter Paragraph to Describe the OMB *Compliance Supplement* Change in Approach for Identifying the Requirements Subject to the Single Audit.** 9110.27 indicates that there is nothing to preclude an auditor from including an other-matter paragraph in the report to communicate information about the change to the supplement. If the auditor considers it necessary to communicate this information, the auditor should do so in a paragraph in the auditor's report with the heading "Other Matter" or other appropriate heading.

Practical Consideration:

For more information, refer to the AICPA website at **www.aicpa.org/interestareas/frc/recentlyissuedtechnicalquestionsandanswers.html**.