THOMSON REUTERS
CHECKPOINT™

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

THE PPC
ACCOUNTING AND AUDITING UPDATE

DECEMBER 2021, VOLUME 30, NO. 12

Private Company Practical Expedient for Share-Based Awards

The FASB issued ASU 2021-07, *Compensation—Stock Compensation (Topic 718): Determining the Current Price of an Underlying Share for Equity-Classified Share-Based Awards (a consensus of the Private Company Council)*, on October 25.

This ASU provides a practical expedient for private companies. It applies to all equity-classified share-based awards issued to employees and nonemployees in the scope of FASB ASC 718, but the expedient isn't available for liability-classified awards.

The practical expedient allows private companies to determine the current price of shares underlying the share-based award using the "reasonable application of a reasonable valuation method," determined at the measurement date.

This ASU was issued to address feedback the FASB received from private companies about the complexity and cost of determining the fair value of options and restricted stock awards at the grant date or upon a modification of the awards.

When using an option-pricing model to determine the fair value of share-based awards, one of the required inputs is the current price input, which is the fair value of the shares that underlie the awards. Because private company shares aren't actively traded and there are no observable market prices available to use, it can be difficult to estimate this input.

ASU 2021-07 includes the following characteristics in its description of "reasonable application of a reasonable valuation method":

- Information considered in the valuation is all information material to the entity's value. A valuation method that doesn't take into consideration all available information material to the entity's value isn't reasonable.
- Factors considered in determining reasonableness include—
  - the value of the entity's tangible and intangible assets.
  - the present value of the entity's anticipated future cash flows.

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™

  - the market value of stock or equity interests in similar entities engaged in substantially similar trades or businesses.
  - recent arm's-length transactions involving the entity's sale or transfer of stock or equity interests.
  - other relevant factors relating to marketability of the stock and the purpose of the valuation.
  - the entity's consistent use of a valuation method to value its stock or assets for other purposes.
- To use a previously calculated value, it must have been calculated no more than 12 months earlier than the measurement date and must be updated for any information available after the calculation date that may materially affect the entity's value.

The Treasury Regulations (Internal Revenue Code Section 409A) use the same characteristics for a reasonable application of a reasonable valuation method for income tax purposes, and this ASU clarifies that it's acceptable to obtain a single valuation to satisfy both requirements. Valuations can be performed by independent appraisers or by the company internally, although the ASU notes that it expects nonpublic entities will often use independent appraisals.

Companies must apply the practical expedient to all share-based awards that have the same underlying share and same measurement date. If they elect to apply the practical expedient, they must disclose the election as part of the minimum disclosure requirements under FASB ASC 718.

ASU 2021-07 is effective prospectively for all qualifying awards granted or modified during fiscal years beginning after December 15, 2021, and interim periods within fiscal years beginning after December 15, 2022. Early application is permitted for financial statements not yet issued or made available for issuance as of October 25, 2021.

Practical Consideration:

The ASU is available on the FASB's website at **www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1176178770358&acceptedDisclaimer=true**.

Auditing Standards Board Issues Risk Assessment Standard

Deficiencies in the auditor's risk assessment procedures are a common issue noted in peer review. Therefore, the AICPA identified risk assessment as an area for enhancing audit quality in 2019.

In October of this year, the Auditing Standards Board (ASB) issued SAS 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*. The standard addresses the auditor's responsibility for identifying and assessing the risks of material misstatement in the financial statements, whether due to fraud or error, at the financial statement and assertion levels. The assessment provides the basis for designing and implementing audit responses to the risks of material misstatements. The effective date will be for audits of financial statements for periods ending on or after December 15, 2023.

SAS 145 supersedes SAS 122, AU-C 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, and amends other sections in SAS 122, along with a number of other auditing standards. It doesn't materially change the concept of audit risk. Instead, it clarifies and enhances the identification and assessment of the risks of material misstatements. It is designed to help auditors determine the financial statement areas that pose the greatest risks of material misstatement, so they can focus more of their procedures in those areas. Among other things, the new standard includes—

- **A revised definition of *significant risk*.** The definition is revised so that auditors will be focused on where the risks lie on a spectrum of inherent risk. The higher on the spectrum of inherent risk a risk is assessed, the more persuasive the audit evidence needs to be.
- **Extensive guidance regarding information technology (IT).** Both the use of IT and the consideration of IT general controls are addressed.

Continued on page 5

The PPC Technology Update

by Roman H. Kepczyk, CPA.CITP, CGMA

Updating Your Backup Strategy

You're sipping your morning coffee as you turn on your computer for the day and rather than seeing your familiar background you have a bright red notice: "Your files are encrypted and can only be unlocked if you pay a ransom." After the initial panic subsides you begin to think rationally: "No problem, I can just restore all my files from my backups."

Think right now . . . How sure are you that your data backups are current, complete, and that you can recover from this scenario (or, for that matter, a fire, theft, or accidental overwriting of critical files)? Compound that with the hasty move to remote computing created by COVID-19. Think about whether current copies of all the work being done remotely is also being properly backed up by your existing system.

Chances are they are not, making it a good time to review your data backup strategy and consider taking advantage of current automated solutions. Today's products not only allow you to restore individual files and previous versions of your entire network, but can also back up remote user data, and even fire up virtual servers in the cloud to be an integral component of your firm's business continuity/disaster recovery plan.

Out with the Old

If you are still relying on physical media—such as a solo network attached storage (NAS) drive, flash drives, DVDs, or even actual tapes—your firm is at risk. These back up types most often require the constant physical intervention of creating and verifying the backups and taking them offsite to a secure location. We often find in consulting with firms that there is seldom consistent follow-through on manual backup procedures, particularly when the person primarily responsible for doing so goes on vacation or there is a staffing change. Modern backup solutions are automatic, verify completeness of the process, and notify firm members if there is a problem or anomaly that requires attention.

Starting with Backup Basics

When evaluating solutions, it's important to build around the basics. Even when utilizing cloud providers, the basic **3-2-1** rules still apply.

- **3**—You should have a minimum of *three* different copies of data (your original production data and two backup copies) in addition to any archival copies you plan to keep.
- **2**—Your copies of data should be stored on at least *two* different types of media (i.e., NAS, cloud).
- **1**—You should have at least *one* copy kept offsite (i.e., secure location, cloud).

Best practices also recommend that at least one backup is *air-gapped* (backup is physically or virtually disconnected from the network) and *immutable* (backup is in a state that it can't be changed in any way). These are features available with modern backup solutions that are designed to counteract a ransomware attack.

Onsite Accessible Images

If your firm maintains servers/data locally, you will want to ensure that any changes are backed up throughout the day. This can be accomplished with on-premises storage devices that automatically create *shadow* copies every 1-2 hours. The benefits of having the *second* copy onsite are that files can be easily accessed and restored when needed, including previous versions, and that they run quickly. These features and many more are more

effectively managed by modern backup applications on NAS or vendor-configured storage devices. However, these on-premises solutions don't protect the firm in the event of a local disaster or theft, which is why an off-site *third* copy is needed, and why firms should evaluate today's integrated cloud solutions.

Backups to the Cloud

Physically moving backup media offsite is fraught with problems, including user follow-through, accessibility, and security. This is why firms should evaluate solutions that automatically backup data offsite via an encrypted fashion. While backing up all files via the internet can take a significant amount of time, modern solutions allow for intermediate backups to be incorporated during the week, with full weekly backups being conducted on weekends to minimize the impact during working hours. Intermediate backups during the week would include *differentials*, which are backups of all files that have changed since the last full backup, making each daily file larger. However, these are quick to restore, as only the full backup and latest differential backup would need to be restored. Intermediate backups can also be incremental. *Incrementals* are backups of all files that have changed since the last backup was made. This means that the full backup and each daily incremental file up to the point of loss would have to restored, taking more time. Modern solutions integrate these different intermediate solutions to more efficiently restore both individual and full system files. The latest solutions also have the ability to restore the data to a virtual environment where the firm can run the applications remotely, similar to how cloud applications and hosting providers function.

Cloud Application Impact on Firm Backups

With more and more applications transitioning to the cloud (think Microsoft 365) or being hosted by cloud vendors that incorporate a comprehensive backup strategy, the internal requirements to back up may be reduced, but still should be verified within the service level agreements of those providers. If the provider cannot meet the 3-2-1 backup rules, firms should take advantage of evolved recovery solutions and consider additional solutions to ensure their client data is adequately backed up. Again, there are modern solutions that allow for faster, more comprehensive backups and live recovery, and firms should evaluate these solutions against the capabilities of their existing systems.

Summary

The threat of a natural disaster, theft, or especially a cyber-attack impacting the information assets and technology within accounting firms has never been as high as it is now, making backups and disaster recovery a priority. Firms should review the capabilities of their current backup processes and compare them to those that are specifically designed to counter current cyber/ransomware threats.

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

- **A new requirement to separately assess inherent risk and control risk.** The risks at the financial statement level potentially affect many assertions because they relate pervasively to the financial statements as a whole. At the assertion level, the risks of material misstatement consist of inherent risk and control risk. For risks of material misstatement at the assertion level, this standard requires a separate assessment of inherent risk and control risk.
- **A new requirement to assess control risk at the maximum level.** If the auditor doesn't plan to test the operating effectiveness of controls, then the assessment of the risk of material misstatement is the same as the assessment of inherent risk.
- **A new *stand back* requirement.** This requirement is intended to drive an evaluation of the completeness of the auditor's identification of significant classes of transactions, account balances, and disclosures.
- **New guidance on scalability.** Auditors must apply their professional judgment to determine the nature and extent of risk assessment procedures required to be performed, based on whether entities have established structured systems, processes, and internal controls and how they are documented. The complexity of an entity's activities and its environment, including its system of internal control, drives the scalability when applying SAS 145.
- **New guidance on maintaining professional skepticism.** An understanding of the entity and its environment, and the applicable financial reporting framework, provides the basis for being able to maintain professional skepticism throughout the audit.
- **Revised requirements on audit documentation.** Audit documentation should include the risks identified, how the auditor obtained an understanding, an evaluation of the design and operation of internal controls, and the auditor's rationale for significant judgments made about the risk assessment.
- **A conforming amendment to perform substantive procedures for each relevant assertion of each significant class of transactions, account balance, and disclosure, regardless of the assessed level of control risk.** Prior to the amendment, auditors were required to perform substantive procedures for all relevant assertions related to each *material* class of transactions, account balance, or disclosure, regardless of the assessed risks of material misstatement.

Practical Consideration:

SAS 145 is available on the AICPA's website at **https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/sas-145.pdf**.

Revised Standard on Review Engagements

In December 2020, the AICPA issued SSAE 22, *Review Engagements*, which supersedes AT-C 210 of SSAE 18, *Attestation Standards: Clarification and Recodification*. SSAE 22 clarifies that the objective of a review engagement is to obtain limited assurance about whether any material modifications should be made to the subject matter in order for it to be in accordance with (or based on) the criteria.

The new standard provides the procedures to be performed in a review engagement, revises reporting requirements to make reports more transparent, and permits expressing an adverse conclusion. It is effective for review reports dated on or after June 15, 2022. Early implementation is permitted only if amendments to AT-C 105, *Concepts Common to All Attestation Engagements*, included in SSAE 21 are also implemented early.

Notable changes covered by SSAE 22 are as follows:

- Procedures should be designed and performed in areas where a material misstatement is likely to arise, based on the practitioner's understanding of the engagement and the subject matter. Review evidence obtained should provide a reasonable basis for obtaining limited assurance to support the conclusion in the review report.

  Inquiry and analytical procedures may be sufficient, but other procedures may be more efficient or effective.

- Review reports are required to include an informative description of the work the practitioner performed to obtain limited assurance to support

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 report conclusion. SSAE 22 permits a brief description, like, "The procedures we performed were based on our professional judgment and consisted primarily of analytical procedures and inquiries," or the review report can provide more detail.

- Adverse conclusions are permitted under SSARS 25, *Materiality in a Review of Financial Statements and Adverse Conclusions*. SSAE 22 requires an adverse conclusion in a review report when the practitioner concludes that misstatements, individually or in the aggregate, are both material and pervasive.

Practical Consideration:

SSAE 22 is available on the AICPA's website at **https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-22.pdf**.