

Public Company *Insights*

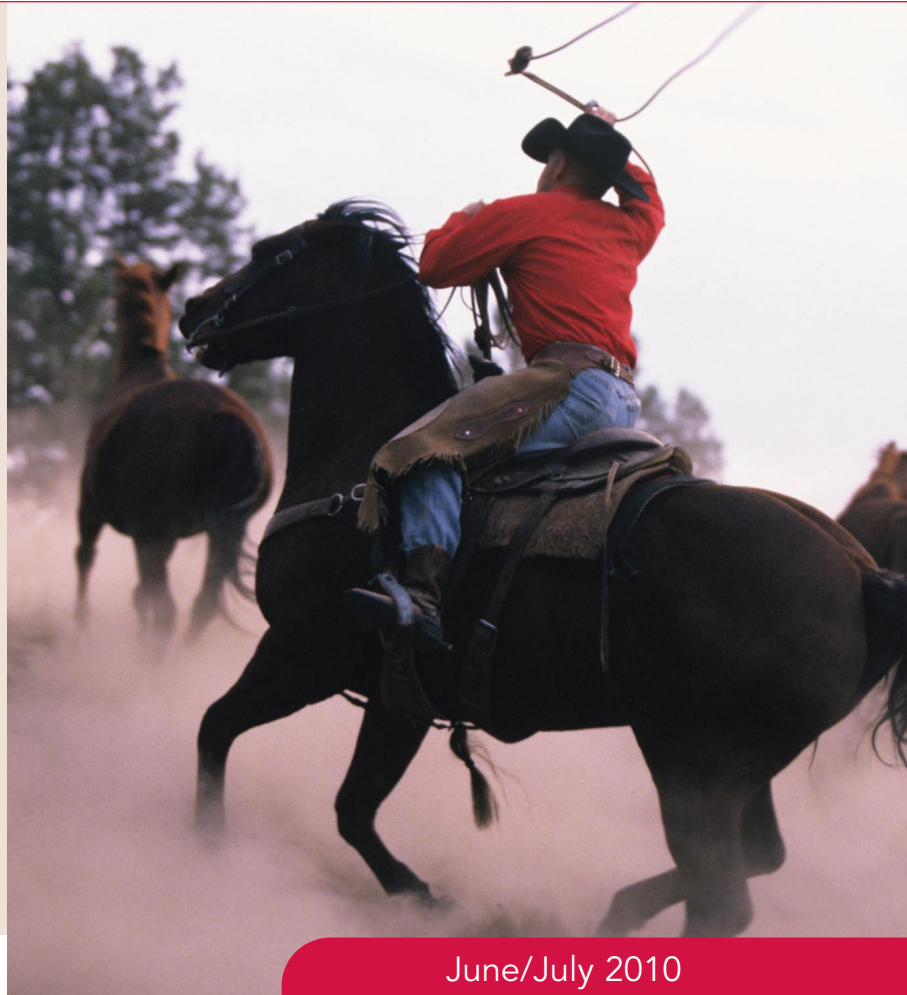
Rounding up
recently released
accounting standards

Building a better audit

New standard requires additional quality review

Does your company meet credit
data security requirements?

Statistical analysis: Your
fraud early warning system



June/July 2010

Rounding up recently released accounting standards

The Financial Accounting Standards Board (FASB) has released a flurry of new standards — and guidance on old ones — in recent years. Some of the changes clarify existing standards, and others strive to converge U.S. Generally Accepted Accounting Principles (GAAP) with International Financial Reporting Standards (IFRS). It's important to review the recent standards and guidance that are most likely to affect your company.

ASU 2010-06: Expanded fair value disclosures

Accounting Standards Update (ASU) 2010-06, *Improving Disclosures About Fair Value Measurements*, requires companies to provide additional details in their financial statements. Such information includes the methods companies use to measure the fair value of certain assets and liabilities.

The update amends Accounting Standards Codification (ASC) Topic 820, formerly known as Statement of Financial Accounting Standards (SFAS) No. 157. Among other things, ASC 820 establishes a three-tier valuation hierarchy based on the types of inputs used to measure an asset's or liability's fair value:

- ▶ Level 1 inputs are quoted prices in active markets for the *identical* asset or liability.
- ▶ Level 2 inputs are observable inputs other than those included in Level 1, such as prices in active markets for *similar* assets or liabilities.
- ▶ Level 3 inputs are unobservable inputs, such as the company's internal data.

In determining fair value, greater weight is given to Level 1 inputs, if available, followed by Level 2 and Level 3 inputs.



The update requires companies to disclose all transfers of fair value measurements into and out of Levels 1 and 2. It also asks companies to provide greater detail about purchases, sales, issuances and settlements related to Level 3 measurements. Companies must further provide disclosures for each class of assets and liabilities, and describe valuation techniques and inputs for both recurring and nonrecurring Level 2 and Level 3 measurements.

ASU 2010-06 generally applies to interim and annual reporting periods beginning after Dec. 15, 2009. The new rules regarding Level 3 purchases, sales, issuances and settlements are delayed until fiscal years beginning after Dec. 15, 2010, and interim periods within those years.

Note that the final version of ASU 2010-06 drops an earlier proposal that would have required companies to conduct a sensitivity analysis and disclose the potential impact on fair value of “reasonably possible alternative Level 3 inputs.” However, FASB may revisit this proposal in the future.

ASU 2010-09: Relaxed subsequent events disclosures

ASC Topic 855, originally issued last year as SFAS 165, established accounting and disclosure standards for events that occur after the balance-sheet date, but before financial statements are issued. Among other things, ASC 855 required companies to disclose the “cutoff date” through which they have evaluated subsequent events. For public companies, this requirement created a potential conflict with SEC guidance regarding the identification and disclosure of subsequent events.

ASU 2010-09, *Subsequent Events – Amendments to Certain Recognition and Disclosure Requirements*, eliminates this potential conflict. It provides that SEC filers need not disclose the cutoff date in their financial statements.

ASU 2010-10: Consolidation of VIEs

In 2009, FASB issued SFAS 166, *Accounting for Transfers of Financial Assets*, and SFAS 167, *Amendments to FASB Interpretation No. 46(R)*. SFAS 167 overhauled the rules regarding consolidation of variable interest entities (VIEs), while SFAS 166, among other things, eliminated the consolidation exception for qualified special purpose entities (QSPEs). Together, the statements make it more difficult for companies to remove certain financial assets or VIEs from their balance sheets.

In December 2009, FASB issued ASU 2009-16 and ASU 2009-17, formally incorporating Statements 166 and 167 into the FASB codification as part of ASC Topic 860 and ASC Topic 810, respectively. The new rules generally apply for fiscal years beginning after Nov. 15, 2009.

In February 2010, however, FASB issued ASU 2010-10, which defers the consolidation requirements for certain interests in investment funds until FASB and the International Accounting Standards Board (IASB) develop joint guidance on consolidating these interests. Such interests include mutual, hedge, private equity and venture capital funds, as well as certain REITs. Deferral of the consolidation requirements doesn't, however, relieve companies of the obligation to disclose these interests.

On the horizon

The Financial Accounting Standards Board (FASB) continues to refine U.S. Generally Accepted Accounting Principles (GAAP) and to work with the International Accounting Standards Board (IASB) to converge U.S. and international standards. The two boards are working together on the following:

Financial statement presentation. This would create a common global format for financial statements. Some of the changes being considered are common categories across the balance sheet, income statement and cash flow statement, and additional details about earnings and cash flows in the footnotes.

Accounting for insurance contracts. Significant changes to the way insurers account for contracts for policyholders are being explored. For example, the boards may eliminate the current practice of deferring policy acquisition costs.

Revenue recognition. This would clarify the principles for recognizing revenue and create a joint revenue recognition standard. The boards expect to issue an exposure draft in 2010 and a final standard in 2011.



Stay on top of trends

Accounting standards seem to be in a constant state of flux. Although it's sometimes hard to keep track of them, many standards will have a significant impact on your company's financial statements, so it's important to monitor FASB and its Emerging Issues Task Force's activities and adjust your strategies accordingly. ■

Building a better audit

New standard requires additional quality review

Earlier this year, the SEC approved a new standard designed to improve audit quality of public companies. Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 7, *Engagement Quality Review (AS7)*, requires more robust concurring or second partner reviews of audit engagements and interim reviews. It applies to fiscal years beginning on or after Dec. 15, 2009.

Second audits?

The new standard's engagement quality reviews (EQRs) aren't intended to be "second audits." Rather, the PCAOB explains, AS7 requires reviewers to "evaluate the significant judgments made and related conclusions reached by the engagement team in forming the overall conclusion on the engagement and in preparing the engagement report." Any additional audit work required for reviewer approval is performed by the engagement team, not the reviewer.



EQRs must be performed by a partner (or equivalent) of a registered public accounting firm. The reviewer must: 1) possess a level of competence qualifying him or her to serve as the engagement partner, 2) be independent of the subject company, and 3) perform the EQR with integrity and objectivity.

To promote objectivity, the standard instructs reviewers (and those who assist them) not to

make decisions on behalf of the engagement team or assume any of the team's responsibilities. It also establishes a two-year "cooling off" period after an audit during which an engagement partner may not perform the EQR for the same company. (Smaller accounting firms, however, are exempt from the SEC's audit partner rotation requirements.)

Robust review process

The PCAOB has explained that these new requirements are necessary to "focus reviewers on the need to perform a robust review, rather than on whether particular matters had 'come to [their] attention.'" To that end, the new standard instructs EQRs to evaluate:

- ▶ Significant engagement-planning judgments, including certain risk and materiality considerations,
- ▶ The engagement team's assessment of and response to significant risks, including fraud and other significant risks identified by the reviewer,
- ▶ Significant judgments regarding 1) the materiality and disposition of corrected and uncorrected identified misstatements, and 2) the severity and disposition of identified control deficiencies,
- ▶ Whether appropriate consultations have taken place on difficult or contentious matters,
- ▶ Whether appropriate matters have been or will be communicated to the audit committee, management, regulatory bodies and others, and
- ▶ Whether the engagement team responded appropriately to significant risks and whether the documentation supports the team's conclusions.

Among items the EQR also is expected to review include the engagement team's evaluation of firm independence, management's report on internal controls, the completion document and the engagement report. The reviewer should further consider information in other documents to be filed with the SEC to evaluate whether the engagement team has taken appropriate action with respect to any material inconsistencies or material misstatements of fact. Similar procedures are outlined for interim reviews.

Clarifying documentation requirements

Under the standard, EQR documentation should "contain sufficient information to enable an experienced auditor, having no previous connection with the engagement, to understand the procedures performed by the [reviewer]." Among other things, the documentation should identify: 1) the reviewer and those who assisted him or her, 2) documents reviewed as part of the EQR, and 3) the date the reviewer provided concurring approval of issuance or the reasons the reviewer didn't provide the approval.

The PCAOB has provided an example of a situation in which a reviewer identifies a significant engagement deficiency. In this case, the EQR

documentation should identify the deficiency, discuss its importance and evaluate the engagement team's response.

To promote objectivity, the standard instructs reviewers not to make decisions on behalf of the engagement team.

Some observers initially worried that AS7 would require documentation of all interactions between a reviewer and an engagement team. However, shortly after AS7 was approved, the PCAOB issued a "Staff Question and Answer" clarifying that the documentation requirements need not be applied until the reviewer determines a significant engagement deficiency exists.

The price of quality

Although the PCAOB has made an effort to avoid turning concurring reviews into second audits, public companies need to prepare for some slight changes in the audit process. Under the new standard, you'll likely use greater auditing resources and may, therefore, experience higher costs. ■

Does your company meet credit data security requirements?

Contrary to popular belief, the Payment Card Industry Data Security Standard (PCI DSS) isn't only for companies that process a lot of credit card payments. PCI DSS establishes minimum requirements for securing sensitive cardholder data, and even one transaction is enough to compel compliance.

The penalties for noncompliance can be severe. They include fines, loss of card-processing privileges and civil damages in the event of a breach. Companies are, therefore, strongly encouraged to review the PCI DSS framework and ensure their organizations meet its requirements.

12 guidelines

The PCI DSS framework contains 12 basic requirements:

1. Install and maintain a firewall to protect cardholder data.
2. Don't use vendor-supplied defaults for system passwords.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data on a "need-to-know" basis.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

10. Monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain an information security policy.

Penalties for noncompliance include fines, loss of card-processing privileges and civil damages.

Companies subject to PCI DSS also must validate compliance with the standard. Validation rules vary depending on an organization's annual processing volume and the credit card issuer's specific requirements.

Getting validated

Generally, companies with the largest number of transactions (typically more than 6 million) must conduct annual onsite assessments using a third-party Qualified Security Assessor (QSA). In some cases, however, they may use internal audit staff. Large-transaction organizations also must have quarterly network vulnerability scans performed by an Approved Scanning Vendor.

Companies with 6 million or fewer transactions are required to conduct annual self-assessments using a Self-Assessment Questionnaire. Depending on the number of transactions they handle, they also must ask an Approved Scanning Vendor to conduct quarterly or annual network scans.

Where to start

If your company processes credit card transactions, it's critical to ensure compliance with PCI DSS. Start by conducting a gap analysis — by completing the Self-Assessment Questionnaire, for example — to determine your current level of compliance. A QSA or other experienced consultant can help you analyze the results.



Keep in mind that the PCI DSS establishes only minimum requirements for data security. The standard requires a firewall, for example, but there are many types and levels of firewall protection. Depending on your company's credit card activities and risk profile, it may make sense to implement a more robust security system than is mandated by the standards.

Indeed, many companies elect to engage a QSA to conduct annual compliance audits even when not required to do so. They typically reason that

the potential consequences of a security breach more than justify the additional cost.

Reputation at stake

Avoiding fines and other penalties is reason enough to make PCI DSS compliance a priority for your company. But there's an even better reason to comply: By securing your customers' credit card data, you avoid liability for data security breaches and potentially irreparable damage to your reputation. ■

Statistical analysis: Your fraud early warning system

Despite implementation of the Sarbanes-Oxley Act of 2002 and other regulatory reforms, fraud remains an enormous problem for U.S. companies. In the Association of Certified Fraud Examiners' (ACFE's) 2008 *Report to the Nation on Occupational Fraud & Abuse*, survey participants estimated that companies lose 7% of their annual revenues to fraud — up from 5% two years earlier. (ACFE was preparing its 2010 report at press time.)

Simple approaches

Auditors use a variety of techniques to detect fraud, including statistical analysis, which can identify anomalies that call for further investigation. Increasingly, companies are using statistical tools internally to detect signs of fraud as early as possible. In many cases, a simple computer program or spreadsheet is all you need.

One effective approach is to search for duplicate invoice numbers or transactions, or even for dollar amounts, which may indicate that numbers have been rounded. More sophisticated fraud detection methods include financial ratio analysis, which identifies trends that may be symptomatic of fraud, and Benford's Law, a tool that can reveal whether numbers have been manipulated.

Data that isn't random

According to Benford's Law, in sets of random data, numbers beginning with smaller digits occur more frequently. Numbers beginning with 1, for example, occur about 30% of the time, numbers beginning with 2 occur about 18% of the time, and so on, down to numbers beginning with 9, which occur less than 5% of the time.

When fraudsters attempt to manipulate numbers in certain financial documents, this pattern becomes skewed. Indeed, it's nearly impossible to manipulate data so that it conforms to Benford's Law.

Applying Benford's Law

To use Benford's Law as a fraud detection tool, you can run a spreadsheet program designed to examine the distribution of first digits in random sets of numbers and calculate the frequency with which the digits 1 through 9 occur. The spreadsheet can be converted into a chart that highlights any significant deviations from the patterns the rule predicts. A chart that shows, for example, that 20% of the numbers in a data set begin with 9 and only 10% begin with 1 may indicate fraud.

However, Benford's Law and other statistical tools don't *prove* fraud. Often, innocent explanations lie behind suspicious patterns. That's why it's essential to enlist the help of a fraud expert when your internal investigations suggest something's wrong with your numbers.

