What are the risks associated with XBRL filings, and what can companies do to reduce their vulnerability?

Risk levels on the rise

When it comes to XBRL (eXtensible Business Reporting Language) filings, vulnerability to risk is increasing for many organizations. Why? The US Securities and Exchange Commission’s (SEC’s) limited liability provision covers an initial 24-month period from a company’s initial XBRL filing. But the provision has already expired for a majority of companies, and it will sunset on October 31, 2014.

Material errors in a company’s XBRL report have the same liability exposures as a traditional, HTML filing. Quality failings are among the most common—and most costly—risks because management is liable for material errors in XBRL filings. XBRL filing errors can be as costly as errors in traditional filings.

Reporting process and control weaknesses may be the most significant risks that management faces. Symptoms of process and control weaknesses include output of reports with material errors, inadequate review procedures, overreliance on automated validation checks, inability to meet deadlines, inappropriate access to systems and data and information technology (IT) controls, lack of understanding of the business and IT controls, reputational risks, and missing documentation.

Another risk is that XBRL-formatted information may fail to comply with the SEC’s EDGAR Filer Manual rules, resulting in missed filing deadlines and/or the need to amend filings.
XBRL: Background and triggers

XBRL is an Internet language designed to facilitate the electronic storage, manipulation, and sharing of business information by making it computer readable. XBRL helps companies by letting information from different sources be easily consumed and analyzed.

Standardized tags (like barcodes) describe and identify each piece of information, which lets various applications sort through the information, quickly analyze relationships between pieces of data, and generate output in multiple formats.

Consequently, financial information can be delivered more consistently—and in a way that is more accurate, more efficient, and less costly and that can enhance flexibility and transparency.

What are the triggers companies should look for?

**Ineffective processes and controls:** Companies may not have fully considered reporting processes and controls with respect to independently reviewing work performed by their outsourcing vendors and may be relying on third-party, automated validation processes that are either incomplete or not sufficiently robust to detect material errors in their XBRL filings. Additionally, there may be gaps in the review process regarding the risks to be avoided in the submission of a high-quality filing.

**Inability to meet deadlines:** Delayed timelines may indicate that disclosure management benefits have not been fully realized. Process and control enhancements may not be fully realized from the company disclosure management implementation. Organizations commonly fail to realize these benefits because of limited implementation scope, inadequate staff training, lack of involvement by reporting professionals, and ineffective change management.

**Inadequate IT controls:** Particularly when a cloud-based disclosure management application solution has been implemented, there may be lack of documentation of disclosure controls and failure to comply with internal IT requirements for data access, backup, and retention. Management should be aware that using cloud-based applications for reporting may not fully protect the company from unauthorized access to sensitive financial reporting documents and data, especially those that are part of the versioning process.

**Inadequate SOX 404 documentation:** Companies may not have fully considered reporting processes and controls with respect to their disclosure management application implementation. Although XBRL is scoped out of Sarbanes-Oxley Act (SOX) Section 404, in many cases those applications are used for processing non-XBRL EDGAR reports certified by management. Management’s assessment of new processes and controls related to its disclosure management application solution may be incomplete and/or inadequate.

---

XBRL is here to stay

Despite the potential exposure, companies usually are reluctant to move forward with initiatives designed to mitigate the risks associated with XBRL filings. Many view an XBRL filing as a regulatory requirement mandated by government regulators who failed to seek input on the real-world impact on those most affected by the regulations.

Further, the SEC has yet to issue any comment letters directly covering these matters, aside from some letters referring to problems with registration statements and the failure to post XBRL exhibits on company websites.

Some executives have the perception that no one is using XBRL, suggesting that reporting risks are relatively low, or nonexistent, or that the XBRL requirement might not remain in place.

But XBRL is here to stay. The status quo stance is a high risk position for companies, considering (1) that XBRL requirements have already attracted the attention of government bodies and (2) the recent sample of a Dear CFO letter sent to registrants around non-compliance with calculation assertions.

Many data analysts are sending emails about XBRL quality and compliance issues in EDGAR to company management, legal counsel, and investor relations, with copies to SEC staff. Also, XBRL is a material consideration in the examination of company financials for issues and anomalies that have the potential to prompt comment letters from the SEC.

How to reduce vulnerability

The best way for a company to reduce its exposure to these risks is to have a comprehensive process in place.

Financial reporting departments are typically understaffed, overworked, and not properly trained in the use of technology and XBRL standards; and some take a go-it-alone approach. In many cases, a company’s most-risk-averse leaders—internal audit and legal counsel—may be more concerned than the financial reporting professionals are with the reporting risks and management liability.

Regardless of the impetus for initiating the process, a company can build a stronger, more-robust XBRL quality program by focusing on the adequacy of its reporting processes and controls.

Common objectives of XBRL-reporting enhancement efforts include:

- Assessing the nature and volume of errors in current- and prior-period XBRL reports
- Determining the adequacy of processes and controls of disclosure management implementation
- Implementing improvements in reporting processes and controls

What’s the right approach?

Building an organization’s XBRL quality process from scratch or enhancing an existing process can be a daunting task. Companies may need help in improving the accuracy, reliability, and reusability of disclosures for users and suppliers of business information while facilitating more efficient communication and analysis.

Companies should center their approaches on:

Training and knowledge sharing:
Deliver both of them based on the company’s particular needs. Training topics might include XBRL overview and background, technical skills, tools training, and compliance and reporting training.

Process and controls:
Assess and recommend on processes and controls over the financial reporting process and integration of XBRL to support the establishment of a comprehensive, controls-based approach to the filing process. The filing process should incorporate taxonomy management, instance creation, and review and submission to the SEC.

Implementation assistance:
Provide support through the implementation of a built-in or disclosure management application. Such support can include project management, process and control recommendations and optimization, and embedding of quality procedures.

Quality services:
Create agreed-upon procedures and comfort letters (completeness, accuracy, consistency, element selection, metadata, table structure, common errors, etc.) and company benchmarking (comparison of elements used in the interactive data filing to peers).
**Contacts**

**Mike Willis**  
Partner  
IT & Project Assurance  
(813) 340-0932  
mike.willis@us.pwc.com

**Tim Pauling**  
Principal  
IT & Project Assurance  
(415) 498-7825  
timothy.e.pauling@us.pwc.com

**Ted Uehlinger**  
Director  
IT & Project Assurance  
(216) 224-5210  
ted.f.uehlinger@us.pwc.com

**James Dreyer**  
Director  
IT & Project Assurance  
(407) 236-5143  
james.h.dreyer@us.pwc.com