

BEST PRACTICES

April 5, 2007

Virtual SOX Compliance

How costs can be lowered

by Bob Benoit and Richard Lanza

Section 404 of the landmark Sarbanes-Oxley Act has been highly controversial since its inception in 2004. Critics argue that the costs of complying with Section 404 exceed the benefits. Advocates point to empirical studies that show SOX-compliant companies had [market beating gains](#) last year. So we know that the costs do not exceed the benefits, but could the costs be lowered? What can we do to drive costs down and vindicate the excellence of controlled growth?

One way is to spend more time on meaningful risk assessments, company-level controls and fraud detection than on less relevant process-level controls. Furthermore, from an IT perspective, many have taken a linear approach to compliance rather than concentrating on internal controls over financial reporting.

But what else can be done besides changing the approach? We believe the answer is virtual SOX compliance.

Paradigm Shift

The concept of performing a Section 404 effort from a remote location requires us to think very differently about how Sox 404 efforts are performed. How could we possibly test the design and operating effectiveness of a company from afar, never mind completely remotely? The key is understanding that SOX compliance is a *management self assessment*. It is not an independent audit. Therefore other members of management can participate in the project as long as their objectivity is not impaired. We can rely on local administrative talent to gather backup documents, scan, upload and observe access controls. This is the first open door to the virtual sox compliance pathway.

The second, is the use of simple and affordable technology tools. For those who have been involved in information technology for a while, the use of remote technology is not a very new concept. What difference does it make if the server is in the next room or in Toronto? Let's illustrate:

Top Controls and Control Design Reviews

All SOX compliance efforts should start with a top-down risk-based approach. This means we start our virtual SOX project with a review of company level accounting controls, COSO components and enterprise risk assessment. Beginning with inquiries of the company's accounting systems, enterprise and fraud risk assessment, control environment, information and communication, we then move to mapping of significant accounts, locations, processes, assertions, use of estimates and selection of accounting principles. The tools we recommend are virtual SOX communities, digital libraries, phones, conference calls and online meeting tools.

Once the above company level controls are documented, assessed and redesigned (if needed), the project can move into the process or activity level control testing phase. This is where the use of technology accelerates:

COMMUNICATIONS:

Teleconferencing, chat rooms and online audio visual meeting tools.

Web cams for more personal communication.

Web-based presentation tools using screen sharing (our machine or the client's machine could be viewed or changed real time).



Richard Lanza



Bob Benoit

Instant messaging.

Share contact lists including the outside auditors.

E-mails for copies of financial statements, spreadsheets, journal entries and disclosure checklists.

DATA COLLECTION AND MANAGEMENT:

Document scans.

VPN connections for screen shots, data integrity testing and access controls.

Screen shots, data integrity testing and access controls.

Version control and access control tools to prevent unauthorized or inadvertent file changes.

Shared site for sharing any documents which is more secure, especially one with SSL certificates. established to encrypt any uploads and downloads to/from the site, so it is the preferred choice.

PROJECT MANAGEMENT:

SharePoint installation (such as Enlightened Technologies) or other Web project management tools such as Basecamp.

Online project management, scheduling and task management tools.

Automatic notification of document updates.

Process Control Lists

The process level, activity level and testing of information technology controls, typically represents the most time-consuming part of a SOX project. It also represents the most intrusive element to company management. Therefore the key to a successful virtual sox compliance effort is the proper selection of a population and sample size. A detailed list of specific transactions, screen shots or control reports to be tested gives the project team and/or management a static list to undertake. A remotely generated and precise list also alleviates much of the inconveniences associated with another group of auditor types pacing the hallways looking for more information. It is essential to ask the right questions however to minimize requests after requests after requests. To generate a comprehensive list of questions, we recommend populating the control matrices and test matrices first. By populating the matrices first, you are assured of broad sweeping coverage of the key controls.

Spreadsheets are most common for evaluating the design and test of controls. Spreadsheets are ideal, particularly in smaller public companies, as everyone knows how to use a spreadsheet and they are flexible enough to be molded to the company's needs. However, for larger companies, this process isn't very secure and can quickly become cumbersome. The benefits of moving the spreadsheets to a database include the following:

Consistency — A database is ideal as it organizes information in a consistent manner. This speeds the review process as people naturally know where to look for their desired data. To further keep the database under control, some companies have decided to move to standard risk and control libraries that are updated by central database administrators.

Quick Searching — Once stored in a database, not only is the information better organized for future action but it also provides a sound foundation for reporting and searching the collective risk management data. The faster searched, the faster control issues are fixed and process improvements emerge.

Security — Some users will need access to all levels of the database while others will only need access to their specific task within the company which may be one control in the database. While such strict levels of security may not be necessary, the right amount of security should be assessed based on the comfort level of the organization.

Risk Management Alerts and Issue Management Workflow — Provides alerts to interested stakeholders in the risk management process depending on new environmental conditions within the business.

Data Analysis

Many SOX control tests can also be performed remotely on a client accounting system via VPN access. Rather than go on site to select samples for example, client accounting data can be accessed remotely. Samples are then selected using audit data analysis tools, and the resulting selection can be communicated back to the client. This can be done without anyone running a report or sometimes even talking to management.

Some controls can be tested 100 percent and remotely using data analysis tools that allow us to look for exceptions within data files. This is useful in the testing of journal entries which are a favorite area for management's estimation and override and therefore a key area for review. Again, using audit-specific data analysis tools, the data can quickly be processed with suspect journal entries selected for discussion with management.

Lessons Learned

The consensus seems to be that virtual sox compliance is the least vexing way to effectively comply with the internal control over financial reporting requirements of SOX Section 404. It also seems to be the most cost effective, even for subsidiaries of major corporations. There are no travel time or travel costs. The remote "testers" are well trained and supervised requiring minimal client interaction. Meetings are scheduled in advance, eliminating the need for ad hoc requests for information. If approached correctly, the right questions are asked in advance, administrative staff are used to their fullest and a top-down risk-based approach is used to generate a right-sized list of internal control recommendations.

However a *completely* virtual sox compliance program is not without its limitations. Good communication is exponentially more important in the virtual sox environment. Very specific requests are needed to minimize back and forth miscommunications. E-mails only go so far — sometimes we have to pick up the phone! Giving management enough time to gather the necessary information is vital for a smooth virtual sox compliance effort. And finally, onsite inquiries should be considered in certain instances. For instance tests of the company level control environment (ethics and integrity) and fraud risk assessments are sometimes best observed in person.

Overall, we found management seems elated with the virtual sox process. Cost effective, efficient and minimal disruption are the highest praises. Seems like a winner!

Bob Benoit, is president of Lord & Benoit, a SOX compliance firm for smaller public companies. Bob serves on the COSO Monitoring Project Task Force, the AICPA Peer Review Acceptance Board in MA, is the author of the Lord & Benoit Reports referenced by SEC, PCAOB, Wall Street Journal, Business Week, all Big 4 firms and over 100 newspapers, magazines, legal, educational and trade journals. Bob's is the first evaluator to use the 2006 COSO Guidance for Smaller Public Companies. He invented several affordable SOX frameworks which can be downloaded from the SEC and PCOAB Web sites or at www.Section404.org

Rich Lanza, CPA/CITP, CFE, PMP, president of Audit Software Professionals, has a decade and a half of experience in the audit and assurance technology field and has become one of its leading authorities. Based on his years in the trenches at several Fortune 500 firms, Rich brings personalized coaching expertise in automating report systems enabling organizations to generate cash recoveries, stop profit leaks, resolve control issues, and implement process improvements. He is a frequent and popular speaker and a prolific writer. His data analysis tool can be found at www.auditsoftware.net.