

How to Survive (and Win) with Sarbanes-Oxley

By Geoffrey James

published on BNET.com 2/26/2008

In 2002, in the wake of the Enron and WorldCom scandals, the U.S. government passed the Sarbanes-Oxley Act, designed to hold public companies to far stricter accounting standards and act as a safeguard against corporate fraud. Among other things, it required independent auditing of a company's finances. On the flip side, "Sarbox" also became a billing bonanza for auditors and an expensive headache for CFOs and CEOs.

But things have changed: In July 2007, the U.S. Securities and Exchange Commission relaxed Sarbox requirements. The new guidelines allow auditors to focus on areas of high financial risk, not every aspect of a company's finances. Below, we'll show you how to navigate the new regulations, choose an auditor, and use Sarbox to reduce redundancies and cut costs. And our article "[Four Reasons to Love Sarbox](#)" will help reset your thinking about the law and how it can be a boon, not a boondoggle.

Things you will need:

- From \$1.38 million to \$11.2 million in external auditing fees, depending on company size. (See "Nitty Gritty," below.) A first-time Sarbanes audit for a pre-IPO company runs double what it will cost in subsequent years.
- About three months to prepare and at least a month (and possibly much longer) for an external audit.
- **External Auditor:** You'll need to hire a CPA firm to audit and certify your financial statements and controls. See Step 3 for how to pick the right auditor.
- **Internal Auditor:** Company finance employees should independently audit financials prior to an external audit so that honest mistakes (or fraud) can be uncovered and expenses curtailed.
- **Top Management Attention:** Your CEO, CFO, and CIO need to make auditing and compliance a priority if you want to drive down the expense of an outside audit.
- **Software Upgrades:** Check with your software vendors (Oracle, for instance) to see if you'll need any upgrades as you shift focus to adding security controls in your existing computing infrastructure.

A yellow sticky note icon with the text 'step 1' written on it in a handwritten style.

Create a Controls-Friendly Culture From the Top

Goal: Lay the groundwork for a smooth audit process.

Ownership of Sarbox compliance should rest with managers who have access to financial controls and the clout to do something about them. "Although internal auditors make recommendations to management, they are not the ones who put policies and processes into place," says Dominique Vincenti, chief advocacy officer for the Institute of Internal Auditors, a professional trade group.

It's also cheaper and easier if managers build controls into their day-to-day activities. For example, instituting a regular policy of changing the passwords to financial systems generally costs less than tracing hundreds of possibly unauthorized accesses after a breach. "Top management should make it completely clear that attention to financial controls is a key element of each group's operational mandate," says J.R. Reagan, vice president and managing director of Global Risk Compliance at BearingPoint. Corporate mission statements, organizational mandates, and individual managers' goals should all make financial controls an absolute requirement. Performance metrics for operational managers should include how well they implement any changes that internal auditors suggest. These steps also protect the reputation of your executives. "If it's clear that a company truly values financial controls, the external auditors will be far less likely to call your corporate governance into question," says Sanjay Narain, a principal with Ernst & Young.

The Legalese

The Sarbox Lexicon

Sarbox: The Sarbanes-Oxley Act of 2002, formerly known as the Public Company Accounting Reform and Investor Protection Act. It created a policing oversight board and banned auditors from doing other kinds of business with clients, such as IT consulting. Sarbox mandated that CEOs and CFOs certify and sign quarterly and annual SEC filings, and it required detailed reporting of stock and off-balance-sheet transactions. The law also imposed stricter internal auditing controls and harsher criminal penalties for fraud.

AICPA: American Institute of Certified Public Accountants. The largest professional organization of CPAs in the United States.

PCAOB: The Public Company Accounting Oversight Board. Created by Sarbox, it registers auditors, defines compliance, and polices conduct.

Section 404: The Sarbox regulation that requires management and external auditors to report on the adequacy of a company's internal controls over its financial reporting. Implementing this can double audit expenses for small to medium-sized firms.

Standard 2: The original guidance from the SEC about how external auditors should approach Section 404. This standard suggested a detailed checklist approach for auditing every financial account, regardless of its relative importance to the overall business.

Standard 5: The new SEC guidance, announced in July 2007, about how external auditors should approach Section 404. It narrows the focus of external audits to high-risk areas of a business and broadly applies to all public companies, although small-cap companies (firms with \$75 million or less in market capitalization) generally face less Sarbox scrutiny.

Evaluate Your Business and Focus on Areas of High Risk

GOAL: Reduce the cost of setting up controls.

A risk evaluation of a company's operation determines which accounts deserve serious auditing attention and which do not. After reviewing operations with the company's internal auditor, management can implement the level of control appropriate for each area of the business.

For example, a VP of manufacturing might do a risk assessment and determine that accounts receivable for raw materials is high risk (because of the high dollar value), the online ordering system for office supplies is medium risk (because everyone has access to it), and in-plant inventory is low risk (because products are shipped within an hour of being manufactured).

In this case, the VP and the internal auditors would determine which controls are adequate and which need further work. Changes might be required to the company's product data management software, for example, in order to ensure that payments for raw materials exactly match shipments.

Technically Speaking

Software to the Rescue?

Software plays a key role in every aspect of Sarbox compliance. Unfortunately, few (if any) companies have the kind of completely integrated computer system that makes it possible to automate the audit. A recent IDC survey of 685 companies revealed that 92 percent use offline data to calculate quarterly revenue reports, which requires manual check by the finance staff.

A number of software vendors — such as Cokato, Minnesota-based Paisley — have emerged with solutions that patch Sarbox-compliant controls into existing software. But such programs can't do much more than create a framework that helps users understand what controls need to be added, according to Tom Eid, vice president of software applications at the Gartner Group. "You can't buy compliance off the shelf," he says. "It's not something that can be shrink-wrapped."

Select the Right External Auditor

GOAL: Find the best fit for your company, and reduce the cost of external auditing.

If your company has executed the first two steps, the actual external audit should go smoothly — provided you hire an external auditor with the right attitude.

Two types of auditors are dangerous: the one that is motivated — implicitly or explicitly — with running up his or her fees, and the auditor with a “gotcha” personality that revels in finding an error your internal guys missed. Avoid these negative types by getting a recommendation from a peer or colleague you trust. “You want auditors who think of themselves as partners in ensuring accurate, compliant financial statements rather than policemen looking only for rules violations,” says Toby Lucich of insidesarbanesoxley.com, an online clearinghouse on Sarbox issues.

Remember that the auditor is taking a risk by agreeing to audit your firm. The mighty Arthur Andersen fell as a direct result of Enron, and CPA firms have not forgotten about the inherent risks associated with their work. Get your CPA on board and keep him or her working for you by involving operational managers in every step of the audit process. “External auditors look for confidence and competence in the companies that they audit,” says Thomas Connors, a partner at auditing firm Deloitte Touche Tohmatsu. “A top-down approach, with management committed to making sure the audit goes smoothly, is the best way to make sure that companies get the most value from the process.”

Checklist

External Auditor Quick-Pick Checklist

We asked Daniel Schroeder, officer of Technology Risk Services at auditing firm Amper, Politziner and Mattia, what to look for in an external auditor. Here are his five must haves:

Qualification. Are they registered with the PCAOB? Don’t laugh. The SEC recently charged 69 accounting firms with violations of this requirement, essentially invalidating their client’s audits.

Experience. Have they conducted comparable audits in your industry, with companies about your size, in the past? Choose a team right for you over a big-name CPA firm.

Track Record. Were those audits cost effective for the client? Get on the phone and check references.

Knowledge. Do they understand your business and industry?

Pragmatism. Can they look at risks realistically and in context? Do they have the maturity to make judgment calls about when to dig deep and when to shrug and move on?

Eliminate Redundancies and Streamline the Audit Process

GOAL: Reduce the ongoing cost of compliance while creating a competitive advantage.

“It’s not at all uncommon for companies to discover that, in response to previous government mandates, they’ve put multiple controls in place that overlap or reproduce the same effect,” says BearingPoint’s Reagan. “Eliminating such controls not only costs less operationally but makes a company easier to audit, because the auditor doesn’t need to check extra controls.”

Management’s focus on risk areas also allows a company to reexamine its financial strategy to make it more efficient. For example, a retail manufacturer might determine that the bulk of the financial risk comes from its factory outlet, which provides a clearinghouse function that could be outsourced. It might make sense in this case to close the outlet, eliminating both the risk and the need to audit that risk.

The goal of Sarbox should be to create a company that runs better, not just a company that complies with regulations, says Deloitte’s Connors. “This is the first time that the government has ever mandated that companies take the entire idea of quality control seriously,” he says. “Ultimately, achieving Sarbanes compliance should be viewed as similar to achieving Six Sigma or TQM — an effort that is as useful and positive for the company as it is for the investors.”

Nitty Gritty

How Much Will It Cost?

The average fee paid to external auditors since the introduction of Sarbox:

	2001	2005	Increase
S&P Small-Cap	\$342,000	\$1,342,000	292%
S&P Mid-Cap	\$650,000	\$2,240,000	245%
S&P 500	\$3,200,000	\$8,400,000	163%

Source: “[The Cost of Being Public in the Era of Sarbanes-Oxley](#),” Foley & Lardner LLP, a business law firm