



Finally, the Party Can Start

It's been five less than satisfying years that companies have had to live with the Sarbanes-Oxley Act, but for the first time there is less fear and loathing and more hope that the new guidance from the SEC and Auditing Standard 5 could turn SOX into something that might actually be a positive for public companies—at least the bigger ones.

From the [July 2007](#) Issue

By [Beth Karlin](#)

But the \$1.12 billion energy products and construction materials company wanted to do it differently. So before it began work on the company's FY2006 SOX drill, Headwaters internal audit staff went to its external audit team with an idea—making Headwaters' 404 audit top-down and principles-based and not a documentation free-for-all. "At Headwaters, we wanted to make SOX compliance part of our normal flow of business," recalls Niel Nickolaisen, Headwaters' director of internal audit. "Our goal was to be fully compliant in as simple a way as possible."

The outside auditors essentially refused, despite the fact that the Public Company Accounting Oversight Board (PCAOB) was already beginning to chastise audit firms for bullying companies into too much testing and too much documentation. Finally, with the help of Headwaters' audit committee, Nickolaisen and Tim Davis, the internal audit manager, won out—unfortunately, not in time to do much with the '06 audit. Even so, the simplification they did push through for that audit and the work they have been able to accomplish in the current year already has allowed the company to slice 25% off the audit time and slash the number of controls tested by a stunning 70%. "We have streamlined the process considerably and cut costs along the way," says Davis.

On the fifth anniversary of the passage of Sarbanes-Oxley, the good news is that the kind of savings achieved by Headwaters and an estimated 10% of pioneering companies, who pursued risk-based audits before regulators officially sanctioned them, will now be available to the other 90% who suffered the tyranny of the 404 paper chase probably longer than they had to. In recent weeks, there has been a collective epiphany about what Sarbanes-Oxley must become—or should have been in the first place—in order to fulfill its original mission to deter corporate fraud and guard against financial misstatements. This past spring the Securities and Exchange Commission (SEC) and PCAOB finally endorsed revised 404 guidance and a new auditing standard—Auditing Standard 5. Together, the new rules call upon companies to focus on the internal controls deemed material to accurate financial reporting in their 404 audits. Auditors were told to accept the judgment of management about how much testing was adequate, unless there were concrete indications that they shouldn't. "The focus has changed from making sure every little box is checked and every door is locked to something a lot smarter," says James Clendenen, engagement director for Parson Consulting, a financial consulting company. "It appears the SEC agreed that rather than taking the shotgun approach and hitting everything on the wall to see what falls off, it's better to focus a rifle on high-risk areas."

This is not to say that all the confusion has been laid to rest—a more exacting consensus on the concept of materiality would, for instance, move the law's self-realization along, as would a more defined role for a company's board of directors when it comes to the threat of fraud by a company's most senior managers. But with a clearer course to navigate, expectations are high for a smoother, less costly set of audits beginning for those companies filing after Nov. 15.

What will the new SOX 404 look like? Experts predict that as it matures, the new SOX internal controls audit will become a piece of a much larger integration of governance, risk and compliance (GRC) by companies—at least that has been the trend at SOX pioneers like Headwaters. "We're definitely at the front end of GRC adoption, and there's no denying that SOX has played a huge

role,” says Scott Mitchell, CEO of the Open Compliance and Ethics Group (OCEG), a nonprofit organization dedicated to defining GRC best practices and methodology. “What Sarbanes taught was that it’s very expensive to have to rapidly respond to an economically significant regulation. Because the pain was so great with SOX, it became a catalyst to not just think about SOX, but think about all areas.”

Best-practices companies like Microsoft Corp. saw the potential opportunity behind the challenge almost immediately. “We had to put a framework in place. We had to document our processes,” explains George Zinn, Microsoft’s treasurer, about the early SOX work at the Redmond, Wash. company. “Then we reworked the processes and reduced the number of controls, so we could be more efficient. Now, we’ve taken what we have done and tried to improve on it so that this is now so much more than just a compliance thing for us.”

Because it requires an enterprise-wide perspective, SOX shines a spotlight on the need for updated financial reporting controls and automation. Says David M. Johnson, a managing director of Protiviti, a provider of independent internal audit and technology risk consulting services, “The best thing about SOX may be that it forced C-suite executives to finally deal out funds for financial reporting upgrades.”

But spending on integrated GRC makes more sense from a cost perspective since SOX is only one of many regulatory compliance efforts companies must juggle and GRC has more direct correlations to performance. “Companies should be taking the SOX effort and viewing it in a wider business context,” says Luc Brandts, chief technology officer and founder of BWISE Inc., a leading solutions provider in the developing GRC software market. “If you take that approach, you can comply with a number of regulations without spending millions on documentation and testing work.”

That certainly was Headwaters’ experience. While its effort began manually, South Jordan, Utah-based Headwaters went the next mile to automate it, selecting BWISE’s GRC management software. Ultimately, if processes are to be flexible enough to expand with a company’s activities and easy enough to repeat each year, some degree of automation must be embraced, many companies like Headwaters have concluded.

Although Headwaters declines to release specifics on its cost savings, OCEG’s Mitchell claims that 30% of the expense of compliance at a poorly integrated, highly regulated industry can be slashed in 12 to 18 months using enterprise-wide GRC. “There is cash waiting to be unlocked,” says Mitchell. “You’re taking what has been historically isolated in silos and starting to integrate it creating efficiencies. And that cuts costs.” Companies in that category, such as financial services, now spend about 15% of revenue for compliance. For industries with less regulation, the expenditure is more like 1%.

Automation also has become more of a necessity in conjunction with SOX testing because of the more explicitly stated emphasis on fraud in the new SOX guidance. “The thing about SOX is that it really targets top management: Ignorance is no longer an excuse,” says Brett Curran, vice president of governance, risk and compliance and privacy practices at Axentis Inc., a provider of GRC solutions. “Over the long run, a dashboard can’t be tampered with as much as an Excel spreadsheet. At every company, there need to be one or more people with influence on board to ask about SOX, and they need to have a dashboard and key compliance and key performance indicators to watch.”

Besides integrated GRC, another discipline that is expected to get a boost from New Age SOX is enterprise risk management (ERM)—although it may take a while longer for large-scale adoption simply because it does not have the same kind of vendor community to push it the way GRC does. While there is no direct link between SOX and ERM, according to consultants, the demands of the law to determine and defend materiality judgments increase the need for the kind of sophisticated identification, quantification and prioritization techniques associated with ERM. “We are in the midst of an ERM boom,” says Lee Dittmar, head of the enterprise governance practice for Deloitte Consulting LLP. “It took a convergence of forces, factors and events that together raised the bar on governance, risk and compliance to bring risk management to the executive suite. I expect an increased focus on better processes, information and enabling systems to help organizations better integrate risk management into their operations and truly address enterprise risks. For most, there is much work to do to reach the goal of being risk-intelligent.”

So does all this mean that the next five years of SOX will be less controversial? Probably, but the critics have not been totally silenced and it is unclear how willingly audit firms will be to go along with marching orders that could cut into their business. “My

concern is that external auditors aren't going to flip in a minute from a bottom-up to top-down approach," says Anne M. Marchetti a consultant and author of *Beyond Sarbanes-Oxley*. "It's going to take a while for that to really evolve into a risk-based approach."

One sore point is that there remains no precise definition of materiality, as used to identify material weaknesses in internal controls on financial reports. That's needed, says high-profile critic Hal Scott, director of the Committee on Capital Markets Regulation and a professor at Harvard Law School, "because a company has to evaluate how much time to allocate to the greatest risks in order to achieve the greatest savings."

This is not a simple task, but Scott presents a possible solution. He recommends a "presumptive, quantitative test of materiality, s that a bad internal control would have to result in a loss of more than 5% of pretax income for the auditors to be concerned with it That would cut auditors' time and, consequently, their bills. In fact, this already appears to be happening.

Even before the new guidance, SOX compliance costs had begun to fall for a variety of reasons—companies had a better grip on the process and, especially the larger or at least more automated ones, began asserting their leverage over auditors who they saw as taking advantage of the SEC's initial scare-them-into-compliance approach to SOX. Phil Livingston, a vice president of Approva Corp., a provider of continuous controls monitoring and audit software, says he has seen outside auditors cut prices as much as 30% in the last year or so. "The Section 404 effort had to be scaled back because it was out of control," says Livingston, who served as FEI's executive director during the earliest years of SOX. "Because if costs didn't go down, Congress would repeal SOX altogether."

A Financial Executives International (FEI) survey this spring found that 200 companies, with an average of \$6.8 billion in annual revenue, saw SOX costs drop an average 23% in 2006 to \$2.9 million from \$3.8 million a year earlier, which, in turn, was a 13% drop from Year One of compliance, when \$4.36 billion was spent.

Another point of contention is that small businesses—those with under \$75 million in capitalization—still bear a disproportionate financial burden in meeting the 404 demands as they are written—even though full compliance has been pushed off for them several times. Currently, set for 2009, the House of Representatives voted in June to extend the deadline for another year. The Senate is expected to consider this issue later this year. "Whatever happens, smaller companies will have the advantage of taking a top-down approach from the start," says consultant Marchetti. "That should minimize their costs."

All the grousing aside, there is one fact that suggests SOX offers companies something more than migraine headaches—even companies that don't have to comply, sometimes choose to. "Some of our clients, especially European clients who aren't even listed on a U.S. exchange, are voluntarily complying with SOX," asserts BWISE's Brandts, "because they see the audit controls bringing order to their operations."

Even more surprising are reports that a lot of companies that are being taken private—and in an era of private equity, there are loads—decide to maintain their SOX compliance operations. Says Microsoft's Zinn, "They want to retain the discipline and continue to build the muscle. They are telling me that they believe SOX is a good tool to have because they might one day go public again, and they wouldn't want to have to start from scratch."

(c) 2007 *Treasury & Risk* (www.treasuryandrisk.com). A WICKS Business Information (www.wbi.com) publication. All rights reserved.