

COMPLIANCE WEEK

Controlling The High Cost Of SOX: Avoid Costly Potentially Fatal Mistakes

By Tim Leech, Special to Compliance Week — Mar. 23, 2004

On Feb. 10, 2004, Financial Executives International released the results of a survey of 321 companies related to total first year costs of complying with Section 404 of Sarbanes-Oxley.

The average compliance cost was \$1.9 million per company. The average cost for large companies with sales over \$5 billion was \$4.7 million.

AMR Research has recently estimated 2004 SOX compliance spending at \$5.5 billion dollars.

In a report released March 3, 2004, Gartner estimated the cost of SOX at between .2 to .4 percent of EBITDA (earnings before interest, taxes, depreciation and amortization). Following a research study done by Gartner Inc. in the fall of 2003, Rich Mogull, research director for Gartner, concluded:

This survey shows that most companies are not leveraging what they have learned from other regulations to achieve best practices for Sarbanes-Oxley compliance. Companies are not addressing the financial requirements for compliance, so they're spending in an ad hoc fashion to piece together a compliance management process. To comply with Sarbanes-Oxley Act and subsequent financial reporting legislation, companies must develop road maps and budgets for formal compliance management processes across their organizations.

SOX Spending Is Out Of Control

Simply stated, Mogull is saying that, in the rush to comply with SOX, many companies have thrown caution to the wind and are spending money without due regard for value.

Ironically, the evidence increasingly supports the conclusion that many companies have "material weaknesses" and/or "significant deficiencies" in their SOX compliance cost minimization controls. As bad as that sounds, the high spending is still producing thousands of SOX compliance frameworks that will not protect CEOs, CFOs and their companies from severe sanctions in the unfortunate event of a serious problem.

Why Are Some Companies Throwing Caution To The Wind To Comply With SOX?

Based on the work I have done with hundreds of companies all over the world related to SOX, the following explanations may apply in whole or part.

1. CEOs, CFOs And Boards Are Scared

Without doubt, the dominant reason many companies are spending with abandon is that the legislation imposes severe penalties at both a personal and corporate level. It is easy for CEOs and CFOs to rationalize high SOX spending to boards of directors. They have personal exposure if the company commits a SOX offense — a federal offense that exposes companies and their officers and directors to jail time and/or fines.

ABOUT THE AUTHOR



Tim Leech is an enterprise risk management veteran who is considered a pioneer in the fields of collaborative

assurance and risk design, having developed software and training for dozens of global companies including Royal Bank, Shell, Georgia-Pacific, CIBC, Mobil, Chiquita Brands and others.

He has held a variety of audit and assurance positions at Gulf Canada Resources (now Conoco) including Manager Special Audit Services, and was also Managing Director of Hambros (UK) Bank subsidiary Network Security Management in Canada.

Leech is the author of several industry books, programs and studies, including "Control Self-Assessment for Risk Management and Other Practical Applications" (John Wiley), and is a regular contributor to London-based [Global Risk Regulator](#).

A former Control & Risk Management Services Director at Coopers & Lybrand Consulting Group in Toronto, Leech is currently the President of [CARD@decisions](#) in Ontario. He can be reached [via email](#) or at (905) 823-5518.

The U.S. Federal Sentencing Guidelines were specifically rewritten in 2002 at the request of Congress to cover SOX. A serious lack of due diligence can multiply fines and jail sentences by a maximum multiple of four. (i.e. one year of jail can become four, a \$70 million fine can become \$280 million) Often this type of situation understandably causes people to forget a key question: We have to comply, but are we doing it in the most cost effective way?

2. **Advisors Using Old Models To Solve New Problems**

Most companies are turning to external auditors for SOX advice and guidance. It will, after all, be their external auditors in the end who assess and report on the acceptability and truthfulness of their SOX 404 representation. The SOX solutions being recommended, at least by some public accountants, come with a high price tag. Richard Lee, respondent No. 17 to the PCAOB Oct. 17, 2004, exposure draft, and a number of other PCAOB respondents, had harsh words for traditional methods used by at least some internal and external auditors in the past:

Unfortunately, internal and external auditors have made internal controls more complicated by engaging in a practice of "documenting controls" that provides very little value, meaning, or relevancy to the day-to-day operations or financial statement reporting integrity of an organization. They have done this because they needed to teach inexperienced staff members how to cost effectively discharge their duties of evaluating business processes of which they have actually very little knowledge or comprehension. The effort to document controls served as an easy way out for the auditors. It ignores the need to assess risk and apply critical judgment to increasingly complex business processes.

They exhaustively documented the existence of internal controls within critical business processes of which they had limited understanding. They deployed inexperienced, often straight out of college, staff members without adequate training or supervision to interview business process owners and to document the existence of controls. They tried to standardize complex business processes into forms and checklists that could be "leveraged" to staff apprentices.

Unfortunately, the type of approach described above when used to comply with SOX Sections 302 and 404 is the worst of all evils. Not only is it expensive, it has repeatedly missed identifying major exposures in the past and has played a part in many of the major corporate disclosure disasters of the last decade.

3. **Execs Want To Claim They Sought Expert Advice**

When faced with a problem that you lack expert knowledge on, it's common to seek advice from those who are supposed to know the answers. We did this ourselves just last week when we needed to install a new server in our office, a job we lacked experience doing.

In the case of SOX, CFOs and CEOs want to demonstrate that they sought expert advice, and reasonably relied on it. But for many companies, this means consulting large public accounting firms, firms that have struggled in the past to develop and consistently apply audit methods that reliably identify serious problems in corporate disclosures.

The bad news is that the SEC has made it abundantly clear that final responsibility for the reliability of external disclosures rests squarely with CEOs and CFOs. The ability to advance a plausible deniability defense for disclosure problems by claiming after the fact that it was done acting on the advice of outside experts, including major accounting firms, is being systematically eliminated by Congress and the SEC.

4. **Companies Want "Easy" Solutions, Little Employee Involvement**

Time and time again we are asked when demonstrating our SOX compliance software where the "magic control checklists" are in the software, checklists that have all the right questions for every possible external disclosure assessment in every industry sector.

Unfortunately, many companies are searching for the holy grail of internal control — magic control checklists that don't even need to be understood by senior management and employees completing them. Just answer the questions, tick yes, no or partial, and move on.

Unfortunately, when evaluating complex automated control systems operated by hundreds, even thousands, of

human beings with limited training in risk and control assessment and often severely conflicted objectives, this approach can lead to disaster. Although it is easy to see the attraction, skipping the age-old question of asking why and taking time to ensure staff understands what needs to be accomplished can, and will, lead to serious personal and corporate exposures for companies of all sizes.

5. Adopting New Technology Impacts Margins; Requires Behavior Change

Survey after survey confirms that many companies are attempting to tackle the complex task of assessing all of their external financial disclosure systems continuously and for the foreseeable future using MS Excel spreadsheets, MS Word templates, and crude — often hastily built — databases. Thousands of public companies are adopting this type of approach, sometimes based on the advice of their external auditors and, at least some, IT strategy advisory companies.

Having worked in this area for more than 25 years all over the world and, perhaps most importantly, being a person who generally dislikes technology, (I still don't know how to operate our VCR), I think I am qualified and entitled to say — in spite of having an obvious conflict of interest as the CEO of a SOX software company — that this advice is just plain wrongheaded and will lead to excessive costs and, more importantly, risks a compliance disaster.

What Should You Do To Control SOX Costs And Manage Compliance Risk?

1. Fully Cost The Money And Time Being Spent On Compliance Of All Types, Including SOX

Our experience suggests that the SOX cost estimates noted in the opening paragraphs of this article are hugely understated. They often do not include many costs being incurred to comply with the legislation and, perhaps, most importantly, do not include the costs flowing from failed compliance efforts. According to a March 3, 2004, Gartner report, HSBC, a major financial services organization, has estimated the total cost of regulatory compliance at 3.125 percent of EBITDA.

The first task when approaching a cost-reduction project including SOX compliance should be to get a handle on what the cost actually is and where is it coming from. This should include the expected SOX compliance costs over the next five years. The next step should be to look for cost reduction opportunities.

2. Get Your External / Internal SOX Advisor(s) To Provide A Comfort letter.

If you are using external advisors in a significant way to help you design and build your SOX 302/404 compliance regime, ask them to document and explain at a macro level their vision of the entire SOX compliance system in Round 1 and in subsequent years.

They should also explain in detail how the SOX compliance system provides a robust due diligence defense under U.S. Federal Sentencing Guidelines in the unfortunate event your SOX compliance system misses a major problem. The senior executive responsible for SOX compliance internally should be asked to complete the same exercise.

The intent of this exercise is to give "comfort" to CEOs, CFOs and the board of directors that the company's SOX compliance system has been carefully designed and implemented and can be relied on. It will also increase the accountability of your internal and external SOX advisors. Those preparing the SOX compliance comfort presentations and letters should be instructed to candidly identify any concerns they have with the ability of the system to comply with SOX and whether cost minimization opportunities exist in future years.

3. Increase Emphasis On Risk And Control Assessment Capability And Reduce Reliance On Control checklists.

The computer system adage "garbage in, garbage out" sums up the reason to ensure all participants in your SOX compliance program understand the fundamentals of risk and control assessment. If you are already using or intend to rely heavily on control questionnaires, formally identify a senior executive in your company and assign direct responsibility for the completeness and appropriateness of the questionnaires.

This step may quickly disclose that very few people are willing to be responsible for a system that relies heavily on "canned" questionnaires. They will be particularly reluctant to take responsibility if there is evidence that the

employees who complete them have only a limited grasp of why the questions are being asked.

4. If You Want To Control Costs, Utilize Enterprise Risk And Assurance Technology That Integrates The Efforts Of All Assurance Providers.

If you haven't done so already, source, purchase and implement a software system that allows all risk and control assurance efforts worldwide to be stored, maintained, quality-assured and monitored in an integrated system.

This system should be COSO ERM compliant and capable of being used for the full range of compliance activities including SOX. It should also be capable of integrating the work of business units and all internal and external assurance providers.

In addition, to be cost effective, this technology should also be capable of linking your corporate policy system directly to the business objectives, risks and/or controls they impact, focusing employees on the costs and benefits of controls, integrating your risk and insurance activities, training staff to complete and maintain reliable risk and control assessments, linking risk and control assessment work to your corporate performance monitoring system, linking to live data in corporate subsystems that indicates risks are escalating and/or performance is improving or deteriorating and more.

The list of software products competing in this area is growing rapidly. Compliance Week hosts a fairly updated list in its [directory of compliance providers](#). The cost of this type of system as a percentage of amounts currently being spent on SOX compliance is small.

5. Utilize An Objective Centric Approach To SOX Risk And Control Assessment.

One of the most common mistakes we see in practice is the use of process-centric approaches that are only loosely linked to specific external financial disclosures. This type of system often does not specifically identify linkages between risks that would cause external financial disclosure to be wrong and the controls in place to mitigate those risks.

This encourages expensive documentation and testing of thousands of activities that are not central to ensuring the reliability of external financial disclosures. The objective-centric approach advocated by the new COSO ERM approach, due out in 2004, should be the primary approach used for SOX assessment work. To do anything less would be to use obsolete approaches with very poor performance track records.

6. Obtain An Independent Assessment Of Whether Your Entire SOX Compliance Program Meets Evolving Due Diligence Expectations.

Regardless of how diligent you are and how much money you spent on SOX compliance, you may still have the misfortune of issuing 10-K and 10-Q reports that contain significant errors and/or omissions.

Once you have designed and implemented your SOX compliance framework you should consider having a macro-level SOX due diligence compliance assessment done under the direction of your legal counsel.

The purpose of this step will be to assess whether you could convince a judge and jury that your company has done the things a reasonable person is now expected to do to prevent financial disclosure problems. You don't want to find out after it is too late that your expensive SOX compliance system is likely to be deemed inadequate, perhaps criminally inadequate. The consequences could be personally and/or corporately disastrous.

The central goal of a well-designed SOX program should be to comply, cover your assets, personal and corporate at the lowest possible cost, and produce the maximum possible benefits to the company.

This is an attainable goal. Good luck.

This column solely reflects the views of its author, and should not be regarded as legal advice. It is for general information and discussion only, and is not a full analysis of the matters presented.

© 2004 Financial Media Holdings Group, Inc. All Rights Reserved.