

COMPLIANCE WEEK

Distilling SOX 302, 404 & 906

By Tim Leech, Special to Compliance Week, May 25, 2004

Since the Sarbanes-Oxley Act was passed in July 2002 hundreds—if not thousands—of articles, white papers and books have been written about the legislation. Most analysts in the field agree that Sections 302 and 404 of SOX are the most complex and costly of what is widely regarded as the most onerous piece of the corporate governance legislation.

Section 302 requires management—specifically, the CEO and CFO—to sign off on financial statement fairness and internal control effectiveness, and has been in full force since August of 2003.

Section 404 requires a separate management report on internal control effectiveness and audit by the financial statement auditor. It becomes effective for large companies starting with years ended after Nov. 15, 2004. Effective dates for smaller companies and foreign companies governed by the SEC commence in 2005.

Section 906 is related to Sections 302 and 404, and requires that CEOs and CFOs ensure all financial reporting—including annual and periodic reports—fairly presents, in all material respects, the financial condition and results of operations of the issuer and that they conform and comply with the Act. It also provides for significant criminal penalties for non-compliance.

Distilling and simplifying SOX 302, 404 and 906 is not easy, and—as is the case with all my Compliance Week columns—readers should not regard this as legal advice, nor should they consider it a full analysis of these complex matters.

Quick History

The Sarbanes Oxley Act of 2002 was passed by U.S. Congress in July 2002, although the SEC has primary responsibility for converting SOX to enforceable rules.

Shortly after the Act was passed, the SEC issued the final rule for Section 302; the Commission issued the final rule for Section 404 in June 2003 (see box at right).

In October 2003, the Public Company Accounting Oversight Board issued an exposure draft of the guidance for companies and external auditors on the standards to be applied for Section 404 audit opinions. This guidance, titled "An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements," was issued in final on March 9, 2004. Also known as Auditing Standard No. 2, it is perhaps the most important of all of these documents, as it is the standard that public accountants must use to audit and report on representations on control effectiveness from public company CEOs and CFOs (also available at right).

Distillation Of The Rules

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.

RELATED RESOURCES

 [Details On The Final Rule Regarding SOX Section 302](#)

 [Details On The Final Rule Regarding SOX Section 404](#)

 [Details, Text Of PCAOB Internal Control Standard](#)

Simply stated, the rules say that CEOs and CFOs of publicly listed companies must be able to demonstrate that they took extreme and unprecedented care to ensure that disclosures in 10-K and 10-Q filings with the SEC—including the numbers, notes, supplemental disclosures, and internal control report and descriptions of significant deficiencies and material weaknesses—are reliable and "fairly presented."

Management must also be able to prove, if required by the SEC and/or the courts, that they met their legal "duty of care" to ensure reliable reporting for at least seven years after certifying each SEC quarterly filing. Specialist staff in public companies governed by SOX and their external auditors should have expert level knowledge of the Act and all applicable rules and related standards.

The Four Pillars Of SOX 302, 404 And 906

To comply with the three sections, companies must demonstrate conclusively that they have four key SOX 302/404/906 "pillars" in place:

1. Macro Level Anti-Fraud Analysis;
2. Macro Level Assessment Against A Control Model;
3. Sufficiency Of IT General Controls; and
4. Reliable 10-K, 10-Q Accounts, Notes And Supplemental Disclosures.

Let's deal with each of these individually:

1. Pillar No. 1—Macro Level Anti-Fraud Analysis

The SEC has stressed the importance of this step, and the PCAOB has made it very clear that external auditors must carefully assess the existence, quality and effectiveness of the controls in place to prevent the issuance of fraudulent and/or misleading external disclosures.

This pillar includes a critical assessment of a range of important anti-fraud controls including the audit committee, whistleblowing mechanisms, codes of conduct, external auditor independence, internal auditors, fraud policy, ethics compliance mechanisms, hiring/firing practices, and much more. The best, and perhaps most stringent, guidance to date we have seen in this areas was issued as a white paper titled [Key Elements of Antifraud Programs and Controls](#)," authored by PricewaterhouseCoopers.

Anti-fraud controls is also a key area of attention for companies that want to be able to demonstrate conclusively that they have met due diligence expectations expected in Section 906 and as defined in the U.S. Federal Sentencing Guidelines. This is particularly true if they want sentence and jail term mitigation in the unfortunate event of a SOX conviction. For example, being able to demonstrate that a strong SOX compliance program was operational during the period may make the difference between a CEO and/or CFO going to jail for three weeks vs. four years and/or the difference between a \$500,000 fine and a \$40 million fine. [Amendments to Chapter 8 of the U.S. Federal Sentencing Guidelines](#) scheduled for enactment later this year raise the standards of care expected by the courts even higher.

PILLAR NO. 1 DISTILLED: The essence of this pillar is simple: Can a company conclusively demonstrate that they took all "reasonable" steps to prevent issuing fraudulent and/or misleading financial disclosures.

2. Pillar No. 2—Macro Level Assessment Against A Control Model

SOX section 404 requires CEOs and CFOs represent that they have an effective system of control in accordance with a recognized control model starting with fiscal years ending after Nov. 15, 2004.

This is a new and radical requirement that the world has only limited experience coping with to date. CEOs and CFOs must opine against, per SEC and PCAOB criteria, a generally accepted control framework—one whose creation follows an exposure draft and due-process procedure. Acceptable frameworks for purposes of this representation arguably include the old COSO framework issued in 1992, the new COSO ERM framework scheduled for release in final in July, the Canadian Criteria of Control framework issued in Canada in 1995 (commonly known as "CoCo"), the Cadbury framework issued in Britain in 1994, the Modern U.S. Comptrollership model issued by the Treasury Board Secretariat of the Canadian Federal Government in 2001, and other frameworks that meet the SEC/PCAOB criteria.

Excellent guidance on how to approach a macro level assessment against a control framework is KPMG's "[Modern Management Practices Assessment](#)" at the Department of Indian and Northern Affairs in Canada. (Modern Comptrollership pilots done in the Canadian federal government since 2000 demonstrate methods to assess the current status of an entity against the criteria in a control model).

The level of guidance in this sample assessment is the type of guidance that the authors of COSO old and new should produce to assist management and auditors. My company (if I may be so bold) has posted a [sample template to assess a macro corporate control framework against the 2003 draft COSO ERM framework criteria](#). I recommend using the new COSO ERM framework scheduled for release this summer for SOX effectiveness representations.

The requirement that CEOs and CFOs opine against a control framework is likely the most problematic of all the SOX requirements at this point in time because the old COSO 1992 framework was not designed to support a "pass/fail" assessment. Further, COSO 1992 and COSO-ERM contain a mixture of control objectives that relate to financial reporting and disclosure and operational efficiency, where "operational efficiency" is outside of the SOX's scope. This just adds to the confusion. The same comments also apply to CobIT re: information technology general controls.

PILLAR NO. 2 DISTILLED: This requirement, although problematic and fraught with difficulty and serious intellectual deficiencies, requires CEOs and CFOs claim that their company has enough of the control elements/criteria listed in the control model they are using to justify claiming they "have an effective control system over external financial disclosures in accordance with (state the control model)."

3. **Pillar No. 3—Assessment Of The Sufficiency Of IT General Controls Over Any System That Feeds 10-K And 10-Q Disclosures**

SEC and PCAOB regulations require that all companies bound by SOX 302/404/906 rules must complete and continuously maintain an assessment of IT general and application controls over any and all systems that provide disclosure information used in 10-K and 10-Q filings. SAS No. 99 and the PCAOB audit standard extend the IT general and application control assessment to include IT fraud risk and fraud detection.

The best guidance issued to date on this requirement is a paper titled [IT Control Objectives For Sarbanes-Oxley](#), issued by the IT Governance Institute.

This SOX 302/404/906 pillar is creating, and will continue to create in the future, significant problems world-wide as many companies have significantly underestimated this requirement. Compounding this problem, there is a limited number of audit professionals with the necessary training and experience to competently form opinions on the adequacy/effectiveness of IT general and application controls over external disclosures.

This requirement will be particularly problematic for the external audit firms that must give SOX 404 opinions, as many of the external audit team members have limited training and experience evaluating IT controls. This is true despite the past requirement in SAS No. 78 for external audit firms to document IT general and application controls regardless of whether they will be relied on or not to reduce the extent of account balance testing.

Many companies have failed to recognize that this assessment must cover any and all automated systems that provide data for 10-K and 10-Q disclosures, not only the general ledger accounting systems. Many of these same companies have also failed to complete fraud risk and detection scenario assessments in their general and application IT control reviews (i.e. sinister intent scenarios).

PILLAR NO. 3 DISTILLED: This pillar fundamentally means that companies have to answer whether there are there adequate controls to:

1. Prevent unauthorized changes to data in software applications?
2. Prevent unauthorized changes to program code that manage and store the data?
3. Ensure programs do what is required and only what is required, and that programs are supplemented by manual user controls where necessary?
4. Control access to assets against unauthorized external and internal use?

4. **Pillar No. 4—Assessment Of The Risks And Controls In Place To Ensure That External Disclosures Are Reliable**

Companies must formally document and maintain assessments of the risks that threaten the reliability of specific external disclosures in 10-Ks and 10-Qs, the controls in place to mitigate those risks, and the acceptability of the current residual risk status (i.e. information on how well the controls are working and the impact of non-achievement).

This can be done using a well designed and continuously maintained compliance-based (i.e. checklist type) approach; a process-centric assessment approach that is specifically linked to all disclosures; or the objective centric assessment methodology promoted by the COSO ERM framework scheduled for release this summer.

The goal is to determine whether there are any reportable conditions in any of these disclosure objectives/processes that meet the definitions of a "material weakness" or "significant deficiency" according to the SEC and PCAOB.

PILLAR NO. 4 DISTILLED: Are there demonstrable risk and control assessment processes and documentation in place to ensure that all—and I mean all!—the information investors might read in a 10-Q or 10-K is complete and reliable.

The House Falls Down If Any Of The Four Pillars Is Deficient

The rules make it clear that if there is even one "material weakness" in any of the four pillars discussed in this article, CEOs, CFOs and external auditors are obligated to conclude that disclosure controls overall are not effective, and must give a negative opinion.

Simply stated: One strike and you're out.

If controls are deficient, it is far better to have management acknowledge the deficiencies in SEC filings and the external auditor agree, than to have a situation where management claims disclosure controls are effective and the external auditor publicly disagrees.

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.