
Regulation Comment Paper Sarbanes-Oxley Section 404

LOBBY THE SEC AND PCAOB FOR CHANGES NOW OR PAY THE PRICE

prepared by:

Tim J. Leech FCA, CIA, CCSA, CFE
CARD[®]decisions Inc.

2655 North Sheridan Way, Suite 150
Mississauga, Ontario, L5K 2P8

Tel: 905 823 5518 Fax: 905 823 5657

Tim.Leech@carddecisions.com www.carddecisions.com

June 18, 2003



Regulation Comment Paper Sarbanes-Oxley Section 404

LOBBY THE SEC AND PCAOB FOR CHANGES NOW OR PAY THE PRICE

Tim J. Leech FCA, CIA, CCSA, CFE

On June 5, 2003 the Securities Exchange Commission ("SEC") released final guidance on Sarbanes-Oxley section 404 titled ***Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports***. In simple language, the new rule calls for CEOs and CFOs to state that they have an "effective" system of control related to external financial disclosures and the company's external auditor to certify the reliability of management's assertion. This new rule represents the SEC's interpretation of section 404 of the Sarbanes-Oxley Act of 2002 ("SOX").

Although the original SEC proposals suggested that the new SOX 404 reporting requirements should entail only a small increase in cost, the SEC now acknowledges that the cost to implement SOX will be significant. External audit fee increases caused by SOX section 404 reporting requirements are expected to be well in excess of 30% on average, with some fee increases well over 100% in the initial reporting period. Many experts are

forecasting that the total cost of implementing SOX will be in the billions of dollars with ongoing incremental costs in the many hundreds of millions of dollars.

The SEC also acknowledged in May 2003 that complying with SOX control reporting requirements is going to be a task of such enormity that they decided to defer the original proposed implementation date for large U.S. companies by at least a year, and for smaller U.S. companies and foreign listed companies by over 2 years. Readers can access the May 27, 2003 SEC Open Meeting webcast at www.sec.gov/news/openmeetings.shtml for more details.

THE KEY QUESTION - WILL SOX SECTION 404 AUDITOR CERTIFICATIONS ADD VALUE AND HELP FIX THE PROBLEM?

Since all the key players acknowledge that complying with SOX section 404 in its current form is going to be an enormous task with an eye popping

price tag, the question everyone should be asking, including the SEC, U.S. Congress, securities regulators, and investors, is "Will the benefits of auditor certified internal control representations from CEOs and CFOs be worth the cost?"

WITHOUT CHANGES - THE ANSWER IS NO

At this point in time, unless there are significant changes in the way the SOX 404 legislation is being interpreted, I believe the answer is no. This paper outlines key flaws in the proposed interpretation and proposes 7 practical and cost effective recommendations to correct the problems.

WITHOUT INTERPRETIVE CHANGES SOX 404 WILL CREATE MAJOR NEW PROBLEMS

In addition to the massive implementation costs, the current implementation strategies will result in:

- a) misplaced investor confidence;
- b) massive increases in Director and Officer insurance costs;
- c) exponential increases in lawsuits against senior executives, directors and external auditors for negligence;
- d) widespread confusion in the ranks of audit committees, senior management, and internal and external auditors related to what constitutes an "effective" control system and a "significant control deficiency";
- e) millions of hours of wasted time preparing control assessments that add little or no value;
- f) massive increases in external audit

fees; and g) very limited positive changes in the corporate control environments of the companies that most need reform.

THE TIME FOR DEBATE IS NOW

This cost/benefit assessment challenges assumptions and conventional beliefs of many regulators and auditors. It has not been arrived at lightly.

My sincere hope is that this article will spur a lively global debate that will lead to amendments to the SEC interpretation of SOX sections 302 and 404 and influence the development of guidance for external auditors by the Public Company Accounting Oversight Board. ("PCAOB")

"EFFECTIVE" INTERNAL CONTROL – WHAT DOES IT REALLY MEAN?

Current interpretations envision a company's CEO and CFO making a statement similar to the following – *Management believes that XYZ Corp maintains an effective system of internal control over external financial disclosures.* The external auditor is then expected to provide an opinion that states *"In our opinion, management's assertion that XYZ Corp maintained effective control systems over financial reporting as of December 31, 200X, is fairly stated, in all material respects, based on the COSO control criteria",* unless their audit indicates there is no support for the management assertion.

On the surface these expectations and assertions appear reasonable. In reality,

both assertions in their current form pose huge problems.

WHAT IS "EFFECTIVE" CONTROL AND HOW MUCH IS ENOUGH?

Without further guidance from the SEC and PCAOB, management assertions on control effectiveness are inherently unreliable.

To illustrate the difficulty with management assertions that state they have "effective" control systems over external financial disclosures, a simple, everyday example related to auto safety can be used.

An objective of most people is to minimize injuries and deaths of passengers and others related to their operation of an automobile. One of dozens of well-known risks to this objective is under-inflated tires. One of the standard techniques to mitigate this risk is regularly checking tire pressure using a tire gauge.

Using this example, if a person elects not to check their tires on a monthly basis, would this deficiency be of such significance that they would be precluded from stating that they maintained an "effective" system of control over safe automobile operation? If they did claim that they maintained an effective system of control over safe automobile operation, in spite of not checking tires at least monthly, would an external auditor be precluded from rendering a positive opinion on the representation? What if tire pressure was checked every four months? What if tire pressure was only checked when

an operator happened to notice a problem? What if the operator's only control in this area is erratically timed, visual inspections of tires, but tests prove that the operator's ability to gauge tire pressure visually without a gauge is very poor?

The problems described in this example apply equally to assessing whether controls related to external financial disclosures are "effective". Without specific guidance on what is "control" and "how much is enough?" assertions on control effectiveness will lead to confusion and misplaced confidence.

ARE AUDIT ADJUSTMENTS EVIDENCE OF INEFFECTIVE CONTROL?

Another more direct example of the difficulty making this type of "effectiveness" assertion relates to adjustments required by external auditors after management has provided their draft set of accounts and supplemental notes for review.

If an external auditor has often required significant adjustments as a result of their audit work, does this fact, in and of itself, indicate that management has not maintained an effective system of internal control over external financial disclosures?

If the answer is yes, my experience suggests that many, many companies around the world have, for a variety of reasons, not maintained "effective" controls related to external financial disclosures. If they had, why would

material changes proposed by the external auditor be necessary?

IS COSO UP TO THE TASK?

The proposed SOX 404 guidance suggests that management should state that “control systems are effective in accordance with the COSO control criteria model or another recognized national control model”.

The five-category COSO control model was developed in 1992. It was a major milestone in the area at that time. The first significant update of the model is now expected in exposure draft form in June of 2003, eleven years after its release.

The COSO framework is a broad set of criteria that the original authors said were important to an “effective” system of internal control. Unlike quality management models like the Baldrige quality framework that is revised annually, has numeric weightings attached to each evaluation criteria, and supporting interpretive guides, the 1992 COSO framework has only very general items to consider when completing a macro level control evaluation, and no guidance at all on how various control criteria should be weighted in arriving at an overall adequacy/effectiveness assessment.

If the criteria used to make control “effectiveness” assertions are vague, how reliable are representations stating compliance with the criteria?

AUDITORS REGULARLY DISAGREE ON "EFFECTIVENESS" GIVEN THE SAME SET OF FACTS

Field research done by *CARD[®]decisions* in countries around the world indicates that it is rare that two groups of professional auditors arrive at the same conclusion on control “effectiveness” using the 1992 COSO control criteria when given the same set of simple circumstances and facts to consider.

If auditors given the same set of facts rarely arrive at the same conclusion, what value will be derived by investors and regulators from an assertion on conformance from a CEO and CFO, and an expensive audit opinion on that assertion from their external auditors?

REPORTING “SIGNIFICANT DEFICIENCIES” AND IN CONTROL SYSTEMS - WHAT'S NEW?

Both internal and external auditors have had an opportunity for over a decade to use the 1992 COSO control framework and other national control models such as CoCo in Canada and the Cadbury framework in the UK to assist them in their work. In light of recent scandals and the scores of reported financial statement restatements following the enactment of SOX, it would not appear to have helped the predictive abilities of many internal or external auditors in identifying “significant deficiencies”. The evidence supports the position that new and improved risk and control assessment tools, criteria, and approaches are required.

WHAT CONSTITUTES A "SIGNIFICANT DEFICIENCY?"

In March 2003, the American Institute of Public Accountants ("AICPA") proposed the following definition of a significant deficiency:

A significant deficiency is an internal control deficiency that could adversely affect the entity's ability to initiate, record, process, and report financial data consistent with the assertions of management in the financial statements.

Although I am a qualified internal and external auditor with multiple professional designations, have decades of auditing experience and provided risk and control assurance training external audit partners and heads of internal audit departments, this definition provides little help when trying to decide which of dozens, or even hundreds, of control issues identified by management and internal audit meet this definition.

Alternatively, given how broad the definition is, a prudent course of action might be to report all or most of the known control issues to be safe. This course of action immediately leads to senior management and audit committees ignoring all or most issues reported, similar to the story of the little boy who cried wolf once too often.

SOME REAL LIFE ILLUSTRATIONS

A simple example to illustrate the difficulty of using the proposed AICPA definition relates to disclosure of pending litigation in the notes to the

financial statements. If research indicates that the conclusions reached by management and their legal counsel related to pending litigation have been materially wrong in 15 of the past 36 SEC 10Q reports, would this indicate that a "significant deficiency" exists in the litigation disclosure system according to the proposed definition? What if the note was wrong in 9 of the 36 reports? What if the note was really, really wrong in 2 of the 36 reports and evidence indicates management knew the pending litigation disclosure had a reasonable chance of being wrong?

If an auditor identifies adjusting entries related to missed or wrong entries in a prior fiscal year that were processed in the accounting records in the current year that totaled more than 5% of the current or past year's income, would this indicate that one or more "significant deficiencies" exist in the external disclosure systems? This situation happens quite regularly.

The 1992 COSO control framework provides little help making decisions on control "effectiveness" and "significant" control deficiencies".

HOW MUCH RISK AND CONTROL TESTING SHOULD BE DONE?

The draft guidance for auditors developed by the American Institute of Certified Public Accountants ("AICPA") issued in March 2003 states that "*The practitioner should **not** rely on the results of procedures performed by others as the principle evidence of the operating effectiveness of controls over*

significant accounts, classes of transactions and disclosures.”

This guidance suggests that, no matter how reliable management assessments and assertions on control status or effectiveness have been in the past, and no matter how much testing of the assertions has been done by Internal Auditors, and regardless of the past reliability of the work done by Internal Audit, the external auditor is required to re-perform testing, at least to some degree, on hundreds, if not thousands, of internal controls.

Whether the new Public Company Accounting Oversight Board ("PCAOB"), the body now responsible for establishing auditing standards in the U.S., endorses this draft AICPA guidance remains to be seen. Guidance on appropriate audit standards for forming a SOX 404 representation and audit opinion is expected from the PCAOB over the next 6 months.

Without changes to the approach taken in the AICPA exposure draft by the PCAOB, companies should prepare themselves for major increases in external audit fees.

WHAT ARE THE REALLY "SIGNIFICANT CONTROLS"?

Current guidance from the AICPA envisions documenting and testing low-level direct controls related to accounting/processing systems. The vast majority of material financial misstatements, both fraudulent and others, were not caused by failure of low-level direct controls in accounting

processes. They were often caused by major frauds and profit manipulations done or directed by senior management and senior level accounting personnel at the corporate level, sometimes on the advice and/or consent of their external auditor.

If the goal is really more reliable external reporting, the risk and control assessment and representations should focus on the truly significant controls. These include the processes in place to assess and report on the quality and reliability of a company's risk identification and mitigation process, controls to ensure that the external auditors are competent and independent, controls to ensure that accounting personnel are competent, rigorous testing of measurement controls which provide information on the current reliability of accounting systems, careful examination of legal counsel correspondence related to contentious and borderline external financial disclosure issues, review of the controls to ensure audit committees are being told which accounting treatments are debatable, testing of the rigor and skills applied by audit committee members to discharge their control governance oversight obligations, and many other truly "significant controls".

Current control documentation and testing frameworks being proposed and offered by a number of control assessment service providers focus little or no attention on the need for this type of "big picture" testing of the real "key controls".

If SOX implementation directions remain unchanged, a substantial portion of the cost of SOX 302/404 implementation will be documenting and testing controls that have rarely been the root cause of the problems that led to the enactment of SOX in the first place.

IF CURRENT PROPOSALS ARE GOING TO COST A LOT, ADD LIMITED VALUE, AND CAUSE MAJOR PROBLEMS, WHAT COULD BE DONE INSTEAD TO ACHIEVE THE DESIRED RESULT?

Given the number and magnitude of problems described above, it might appear at first glance to be an insurmountable challenge to implement SOX 302/404 in a cost effective way and still achieve the goal of improving the reliability of external financial reporting.

This is not the case.

With some adjustments to the way the SOX legislation has been read and interpreted to date by the SEC, and some carefully constructed guidance from the PCAOB and SEC, the aims of SOX 302/404 can be achieved, and achieved at a cost that would be more than justified by the benefits. Suggestions on how to accomplish this follow.

RECOMMENDATION #1
Agree on a practical definition of a "significant control deficiency"

A key step is to reach agreement on a workable definition of a "significant control deficiency", the items that should

be reported to the external auditor and audit committee. The definition should be as simple as possible but still capable of capturing material unmitigated risks. An example of a definition that reflects more current risk-based thinking is:

"A significant control deficiency is a situation where, in the opinion of management and/or internal audit, one or more risks are not mitigated to an acceptable level and threaten, in a material way, the goal of reliable external financial disclosures".

RECOMMENDATION #2
Encourage companies to implement automated, real-time enterprise risk and control assessment systems

To keep the cost of SOX 302/404 compliance contained over the longer term, and maximize benefits from the new activity, the use of software that incorporates all risk and control documentation, assessment, and testing should be encouraged. New software vendors are entering this field in response to SOX on a monthly basis. Major improvements are being made to the capabilities of these systems.

SEC guidance provided on May 27, 2003 related to auditor independence suggested this technology should not have been developed or sold by the external auditor that will be reporting on senior management's SOX 404 control representation. This relatively clear position was altered with conflicting guidance issued on June 5, 2003 in the Final Rule.

Regardless of who the software vendor is, the software used should be capable of assessing both "big picture" risks as well as assessing risk status in the significant external disclosure systems.

Readers can find more details on how to complete a technically sound risk and control assessment and the new SEC SOX 404 independence interpretations at <http://www.carddecisions.com/sarbanes-oxleylinks.html>

RECOMMENDATION #3

Assess, score and report on the organization's risk management system related to external disclosures

The new 2002 Institute of Internal Auditor ("IIA") professional standards require that internal auditors report on the reliability of their client's risk identification, measurement, mitigation, monitoring and reporting systems. For purposes of SOX, this assessment should focus on the processes that feed and support the company's external disclosures.

The IIA has published guidance on how to develop this type of opinion in their landmark guide "Implementing the Professional Practices Framework". The 2003 COSO exposure draft now expected in July 2003 should also increase the focus on this area.

The risk assessment system evaluation framework should utilize a weighted set of criteria that will allow a numeric or alpha grade of "risk fitness" or "risk management capability" to be reported to senior management, the audit

committee and the external auditor. This score indicates the capability of the organization, on a timely basis, to identify, measure, react to, and report on significant risks that are, or could, threaten the reliability of external disclosures.

Scoring an organization's risk fitness is far more transparent and amenable to objective assessment than a highly subjective "control effectiveness" opinion.

RECOMMENDATION #4

Focus on assuring investors that significant, unmitigated risks are being identified and reported to audit committees and external auditors on a timely basis - not on deciding what constitutes "effective" control

Instead of requiring the CEOs and CFOs assert that they have "effective" controls over external disclosures, the SEC and PCAOB should mandate representations from CEOs and CFOs stating that there is an effective system in place to identify and report significant unmitigated risks to the company's audit committee and external auditors. A sample management representation is included as Attachment 1.

The company's external auditor should provide an opinion on the reliability of that assertion by auditing the system in place to identify, measure, mitigate and report on risk and control status related to reliable external disclosures. A sample external audit representation is included as Attachment 2.

This approach avoids the problem of attempting to assess what constitutes "effective" using the vague, unweighted control models that currently exist, is more practical and cost effective, and correctly positions the job of assessing the acceptability of major risks related to external disclosures with the company's senior management team, audit committee, and the company's external auditors.

Most importantly, if the risk identification and measurement assessment criteria are properly defined, it focuses attention on the big picture risks to reliable external financial disclosures, not low level accounting controls that are rarely the root cause of big problems.

RECOMMENDATION #5
Let external auditors do what they are trained and paid to do – decide if control deficiencies preclude reliable disclosures

If investors and regulators can be assured that there are reliable systems in place to identify and report serious risk and control issues to audit committees and external auditors; external auditors should then be in a much better position to make a professional determination as to whether one or more reported, significant unmitigated risks preclude providing a positive opinion on a company's external financial disclosures.

External audit partners usually have at least a decade of experience to help them make this type of decision. They are specifically trained for this, and carry

errors and omissions insurance in the event evidence indicates that they made the determination corruptly or negligently.

RECOMMENDATION #6
Lobby the IIA and the PCAOB to provide new and better guidance on what constitutes a "key" control

Management personnel, regulators, internal and external auditors need new and substantially better guidance on how to assess and report on the state of risk and control. In particular, the guidance should stress the critical importance of identifying, documenting and testing the reliability of Measurement/Indicator controls.

Measurement/Indicator controls are controls that provide information about the reliability of external disclosure processes at both the macro and more micro levels. These controls should be considered to be "key" controls because they provide information on the current effectiveness of all other controls in the control design.

Although the idea of focusing on key performance indicators ("KPIs") has been embraced, studied, and used by the quality movement for many decades, only a small number of internal and external auditors have employed this technique in a significant way to assess and report on risk and control status to senior management and audit committees.

Senior management and audit committees should be told which financial disclosure processes have high

error rates and low reliability. Macro level controls described earlier in this paper in the section titled "WHAT ARE THE REALLY SIGNIFICANT CONTROLS?" should also be classed as "key" controls.

RECOMMENDATION #7 Dedicate More Resources to Evolving and Refining Generally Accepted Control Criteria ("GACC")

Waiting a decade between major reviews and updates of the COSO control framework is unacceptable if the COSO model is going to be used as the foundation for the new global "Generally Accepted Control Criteria". ("GACC")

Companies and internal and external auditors should lobby the COSO founding members to dedicate resources to evolve the sophistication and rigor in the COSO control framework. The current COSO website, www.coso.org, requires a major overhaul and ongoing maintenance given the elevated importance COSO will now have in light of SOX 404 requirements.

The control criteria in COSO should be numerically weighted in terms of importance, the evaluation criteria refined, the model should be updated based on experience and user input at least every 3 years or after every major governance failure, and money should be contributed to ensure a robust maintenance and continuous improvement process is in place.

INACTION WILL BE COSTLY

The time to lobby the SEC and PCAOB for change is now. If SOX 302/404 implementation follows the path it is currently on, it will create more problems than it solves. The huge escalations expected in director and officer insurance premiums and external audit fees and the massive cost to implement this new regulatory regime in its current form will further burden the global economy. Good regulation should solve more problems than it creates.

LET ME KNOW WHAT YOU THINK

This article has laid the reasons why I think the current plans to implement sections 302/404 are not cost effective and will not succeed in addressing the problems SOX was created to address. Seven recommendations have been proposed to redirect the regulatory implementation of SOX 302/404 to obtain maximum possible societal benefits.

I would like to hear from you. Send your comments, both positive and negative, to me at tim.leech@carddecisions.com. I will post all comments received on our website, www.carddecisions.com in the Industry Info/Sarbanes-Oxley section.

Tim Leech is founder and CEO of CARD[®]decisions Inc. based in Mississauga, Ontario, Canada. CARD[®]decisions specializes in risk and control governance training and technology.

Sample Management Representation to Audit Committee

We, the undersigned, acknowledge to the Audit Committee that we have:

- (1) Responsibility for developing and maintaining internal controls and disclosure controls that provide reasonable assurance that ABC's financial statements and supplemental SEC disclosures present fairly the results of operation and the financial position of ABC Inc. in accordance with generally accepted accounting principles and other applicable SEC regulation.*
- (2) Responsibility for overseeing that the organization has cost effective risk and control management systems that provide reasonable assurance ABC's external disclosure objectives will be achieved.*
- (3) Reviewed the significant control and risk issues identified by work units and management through the company's risk and control self-assessment process, and the significant issues identified by our Internal Audit department and our External Auditor, Smith & Jones, that have been brought to our attention. We have initiated steps to adjust controls in areas where the error rates and/or residual risks identified related to the non-achievement of ABC's disclosure objectives were considered to be excessive and/or unacceptable.*
- (4) Reviewed our process to manage risks and internal control and this year's report on our risk management process prepared by our Internal Audit for the Audit Committee. We are satisfied that our risk and control assessment framework process provides you, our Audit Committee, and our External Auditors, Smith & Jones, with a reliable and materially complete report on the risk and control status related to our external financial disclosure objectives as required by sections 302 and 404 of the Sarbanes-Oxley Act of 2002.*

CEO

CFO

Sample External Auditor Representation

Management of ABC Corporation are responsible for:

- (1) designing and maintaining an internal control system to provide reasonable assurance regarding the reliability of external financial disclosures;*
- (2) designing and maintaining a risk management system related to reliable external financial disclosures that is capable of identifying significant, unmitigated risks that threaten the objective of reliable external financial disclosures;*
- (3) designing and maintaining an effective system to escalate significant control deficiencies in the external financial disclosures systems to the company's audit committee and to Smith & Jones, the company's external auditors.*

*We have completed an audit of the system in place to identify and escalate significant control deficiencies in the external financial disclosure system in accordance with **Generally Accepted Audit Standards** specified by the Public Company Accounting Oversight Board.*

In our opinion, the risk identification and escalation system related to reliable external financial disclosures provides reasonable assurance that significant control deficiencies are being escalated to the company's audit committee and to us, Smith & Jones, the company's external auditor. We utilize the information on external financial disclosure control deficiencies when forming our audit opinion on the reliability of the company's external financial statements and note disclosures.

Smith & Jones

Date