

February 26, 2007

Mr. Christopher Cox  
Chairman  
Securities and Exchange Commission

Mr. Mark W. Olson  
Chairman  
Public Company Accounting Oversight Board

**RE: IMA SECOND SUBMISSION SEC FILE No. S7-24-06 and PCAOB Rulemaking  
Docket No. 21 (Focus on Risk-Based)**

**EXECUTIVE SUMMARY**

The Institute of Management Accountants (IMA) has carefully reviewed the current SOX proposals put forth by the SEC and PCAOB in December, 2006 and we respectfully believe that they constitute a material weakness for investors, businesses and U.S. global competitiveness. As used in the proposals, the term “risk-based” is not consistent or in accordance with generally accepted global risk management principles. IMA bases its conclusions on 2 years of practical research, an exposure process with its 65,000 members, a review of comment letters already filed by organizations representing large investor and business communities, and testimony at the February 22, 2007 PCAOB Standing Advisory Group (SAG). The IMA is very concerned that the SEC and PCAOB are not taking advantage of global risk management approaches and are not complying with the ISO standards for national regulators. This is not an academic concern – misuse or lack of use of market-tested risk management approaches will perpetuate materially incorrect financial statements, high costs, increased profits and potentially crippling litigation risk for the audit firms, and continued reluctance of high growth smaller companies to participate in U.S. capital markets.

It is possible to correct this situation if the SEC and PCAOB are willing to consider and incorporate true risk-based disciplines and frameworks put forth by IMA, COSO, ISO and other globally recognized organizations with significant investor and business constituencies. With respect, the PCAOB proposed standard is still fundamentally audit and control-centric (relying on decades old audit perspectives) and perpetuates the power imbalance for auditors. The SEC proposed guidance is not risk-based by any existing global risk management standard and is too ambiguous to be practical for assessment purposes, especially for smaller public companies.

**BACKGROUND/TECHNICAL COMMENTARY**

IMA filed its primary comment letter with the SEC and PCAOB on February 13, 2007. On February 20, IMA senior staff met with nine SEC and PCAOB staff who participated in the drafting of the exposure drafts to answer questions on our comment letter. On February 22 we listened carefully to the PCAOB Standing Advisory Group Meeting in Washington via webcast.

Upon reflecting on the research we have completed, research done by Glass, Lewis & Co, the meeting with your staff last week, and comments made during the PCAOB SAG webcast, it has become very clear to us that the use of the term "risk-based" is a major problem. This is a problem that will, if not addressed, lead to continuation of massive unnecessary SOX compliance costs, resistance to the adoption of section 404(b) from non-accelerated filers, continued inability to properly address senior executive directed fraud, erosion of U.S. competitiveness, and continuation of an unacceptably high incidence of audit opinion failure.

IMA's February 13, 2007 comment letter on the exposure drafts takes the position that the term "risk-based" should be interpreted in the context of globally understood risk management terminology and use. In the current regulations and the exposure drafts the meaning attributed to "risk-based" is not consistent with what the risk management community considers to be "risk-based". The meaning and application of the term risk-based is, in the words of a number of the speakers at the PCAOB SAG meeting, "the same thing we've had for the last two decades" – the same audit approaches that have failed in an alarmingly high number of instances over the past two decades.

Lynn Turner, Managing Director of Research, Glass Lewis and former SEC Chief Accountant indicated at the PCAOB SAG meeting that the current interpretation of "risk-based auditing" is one that it is written "by auditors, for auditors". His conclusion appeared to be that the current interpretation in the SOX regulations of "risk-based" is pretty much "the same thing we've had for the last two decades". Mr. Turner's summary conclusion on the current PCAOB interpretation of "risk-based" is that it represented "a gaping hole in this particular document" (PCAOB ASX/5).

The ISO Guide 73: *Risk Management - Vocabulary – Guidelines For Use In Standards* is specifically intended to be used by regulators when creating standards that relate to risk management.

*The Guide provides standards writers with generic definitions of risk management terms. It is intended as a top-level generic document in the preparation or revision of standards that include aspects of risk management.*

*The aim of this Guide is to promote a coherent approach to the description of risk management activities and the use of risk management terminology. Its purpose is to contribute towards mutual understanding amongst the members of ISO and IEC rather than provide guidance on risk management practice.*

The term "risk-based", as interpreted over the past 30 years by external auditors and audit standard setters, has focused on audit risk and techniques to minimize the chance of providing a wrong audit opinion. The emphasis is on subjectively identifying "risky" locations, processes and accounts. With respect, we don't believe that this brand of "risk-based" auditing methods has been effective at a level consistent with stakeholder expectations, particularly in the area of fraud prevention and detection.

A number of participants in the PCAOB SAG meeting last week remarked on the generally negative perception of the term "risk-based" created by some auditors, auditors that interpreted in the late '80s and '90s the term to be a ticket to reducing audit work and permitting the acceptance of the premise that all senior management teams are honest and well-intending.

The audit community lexicon for the term "risk-based" and, most importantly, the interpretation in the current SEC and PCAOB exposure drafts, does not require that management or auditors explicitly identify and measure known risks that threaten the reliability of the financial statements.

Specific examples of fraud-related risk that should be explicitly identified and assessed include:

1. CEOs and CFOs have significant financial incentives to falsify and/or inappropriately manage financial results.
2. Management has major financial incentives to direct backdating of stock options.
3. Senior management directs improper/fraudulent post-close journal entries to manage profits.
4. Management override of controls.
5. Audit Committees have financial incentives not to ask the tough questions.

The list can easily be extended using examples from thousands of recorded instances where auditors were misled by unethical and fraudulent senior management. A true risk-based analysis of ICFR would be expected to specifically identify the controls in place to mitigate these types of risks, as well as the more benign simple error type risks and assess their likely effectiveness. The emphasis to date, and a large percentage of the costs, has been on the benign risks - not on the truly dangerous risks that led to the enactment of SOX and erosion of investor confidence.. Separate and expensive forensic fraud audits of every public company are not necessary. Correct interpretation of the term "risk-based" and application of true "risk-based" assessments using tried and tested risk management methods by both management and auditors is necessary.

The evidence IMA has gathered during its research indicates that very few registrants, and even fewer auditors, are explicitly identifying, documenting and directly assessing the controls in place to mitigate the type of very predictable fraud-related risks listed above. The regulations also do not require that management and auditors explicitly identify and monitor the acceptability of what is known in globally accepted risk management vernacular as "residual risk", the risk remaining after risk treatment. In the context of ICFR, this is the error rate detected by management and external auditors in all accounting and disclosure processes that feed public financial disclosures.

Measurement of error rate is a key component of any good risk management system, a cornerstone of the global quality movement, and widely associated with the well known expression "WHAT GETS MEASURED GETS DONE". In the quality profession, whether you apply the principles of the ISO 9000 system, the U.S. Malcolm Baldrige quality system, the core principles of Six Sigma, or the core operational requirements of the Basel II reforms in banking, not tracking and analyzing detected errors would be tantamount to a material weakness in a quality system.

IMA research confirms that a significant percentage of accelerated filers during the first two SOX reporting cycles did not identify and evaluate specific risks that threaten the financial statements at the entity level, and, perhaps most importantly, did not identify fraud specific risks. These research findings are contained in the IMA 2006 research study *Internal Control: COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices*.

**THE PATH FORWARD**

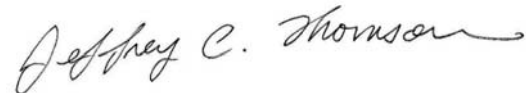
IMA strongly believes that a more “investor friendly” approach relative to current proposals is for the SEC and PCAOB to seriously address what Lynn Turner termed a “gaping hole” in the current exposure drafts. Proper understanding and application of market-tested global risk approaches will better protect investors and give businesses of all sizes the flexibility and accountability to grow investor wealth.

IMA, as a not-for-profit organization devoted to providing professional development and the CMA certification to the global management accounting community, will continue to provide a solutions-orientation to assist the SEC, PCAOB and other bodies in improving SOX compliance. We have provided the following resources to the SEC, PCAOB, U.S. Chamber of Commerce, the Small Business Administration, COSO, corporations, and other organizations which are also available at no charge on the IMA website [www.imanet.org](http://www.imanet.org): 9/15/06 IMA Comment Letter to the SEC which describes in detail a risk-based framework and other solutions; 1/17/07 SMA (Statement on Management Accounting) which describes the fundamentals, global frameworks and principles underlying Enterprise Risk Management; and, the 2/13/07 IMA Comment Letter to the SEC and PCAOB which describes our “five point plan” to improve SOX compliance for investors and businesses of all sizes.

Sincerely,



Paul Sharman  
President & CEO



Jeffrey Thomson  
Vice President of Research