Arnold Schanfield, CIA, CPA
1481 Center Avenue
Fort Lee, NJ 07024
201-207-7935
aschanfield@verizon.net

December 10, 2013

Office of the Secretary, PCAOB
1666 K Street, N.W.,
Washington, DC 20006-2803
Subject: PCAOB Release No. 2013-005/ Rulemaking Docket Matter No. 034

Dear PCAOB Board:

Please find my commentaries below on the two proposed auditing standards "The auditor's report on an audit of financial statements when the auditor expresses an unqualified opinion" and "The auditor's responsibilities regarding other information in certain documents containing audited financial statements and the related auditor's report."

We understand from Page 2, your comment "that the auditor's report in the United States has changed very little since the 1940s and that the existing pass/fail model is thought by many to be useful, because it provides a clear indication of whether the financial statements are presented fairly." In my opinion and that of many highly qualified risk management practitioners and especially those from outside of the United States, the auditor's report has had serious deficiencies for a long time and as such, I reject the notion that the financial statements present fairly, as most of the major business risks that a company incurs, evolve from the strategic planning process and not the financial statements. The financial statements are one of the culminating documents from the strategic planning process.

As an example of the above, British Petroleum (BP) to date has paid out some $42.5 billion in penalties, fines and claims related to the Macondo oil spill in the Gulf of Mexico in April 2010. It is fair to say the external auditors focused on the financial statement audit prior to the spill but completely ignored the strategic plan/objectives and most of the critical risk management aspects of the company. The way that the external audit and Sarbanes Oxley in particular are conducted, is a "top down" risk assessment but top down in the context of the financial statements. This is consistent with the COSO Internal Control Framework and with AS5. A risk assessment following the guidelines of ISO 31000 and further the implementation guidelines of HB 436 from Australia as well as leading practices in Canada and the United Kingdom, commences from the strategic objectives.

The bottom line is to identify the uncertainties that could impact the business objectives of the company, upon giving consideration to the company's stakeholders. It is the analysis of such uncertainties for likelihood of occurrence and significance to the company's business objectives, which produces the risk. In the case of BP, it is unlikely that both management of the company and its external

auditors, clearly identified the potential for a major spill as an uncertainty and thus a risk. The test of this is whether there would have been an accrual on the balance sheet for this pending disaster. We know that under existing generally accepted accounting principles, there was no such accrual and yet there was a major risk. This comprised a risk clearly not identified by the external auditors and as well by the company's risk management system and internal auditors.

For many years now, the external audit has been broken primarily evidenced with the Enron debacle and the subsequent roll out of Sarbanes Oxley. Use of the COSO framework as the backbone of Sarbanes Oxley was a huge mistake because this internal control model was constructed built on a flawed interpretation of the financial statement risks. It considers the "game" to be opining of the financial statements when the "game" is providing assurance to a wide variety of stakeholders. There were more suitable internal control/risk management frameworks available than COSO.

Unfortunately, in the United States unlike the United Kingdom, Canada and Australia/New Zealand, research in risk management was outsourced to the large accounting firms and their agents. So what exists in the United States is a product by the public accounting profession for the public accounting profession instead of a product produced by worldwide experts in internal audit, control, risk management and governance for use by all companies.

Just prior to the Enron disaster, there already existed in the marketplace leading internal control, risk management and governance frameworks from the countries of Canada (CoCo-1995; QSA 850-1997); United Kingdom (Turnbull, Cadbury, Combined Code) and Australia/New Zealand (AS/NZS 4360:1999). Such guidance was ignored and instead, COSO was rolled out as the backbone to Sarbanes Oxley and then we witnessed introduction of COSO ERM in 2004 (also flawed). Simultaneously to COSO ERM, was the introduction world wide of the third edition of AS/NZS 4360(2004) from Australia/New Zealand, which served as the foundation for issuance of ISO 31000 in 2009. Enron was not a disaster on financial statement fraud. It was about corruption, tone at top issues and greed. A well constructed risk management program including an independent review of board performance, would have impeded significantly, issues resulting in the collapse of Enron. The internal control model represented by COSO is quite deficient and the COSO ERM framework is just a further representation of this deficiency.

The turbulence created as a result of such deficiencies in the framework being used and continued marketplace disasters, allowed for a variety of other non value services to be created such as GRC in 2003. When you analyze precisely what these materials contain, you will in the best possible scenario walk away with the impression that there is further distraction from the main issues that companies needed to be dealing with. In no other major English speaking country other than the United States, would this have been possible. In addition, the plethora of vendors hawking software which purportedly will manage risk, is staggering. None of these however, are founded on robust established principles of good risk management.

So when you state on page six of the release, that "the auditor's required communication would focus on those matters that the auditor addressed during the audit of the financial statements that involved the most difficult, subjective, or complex auditor judgments or posed the most difficulty to the auditor

in obtaining sufficient appropriate audit evidence or forming an opinion on the financial statements", I think that you are missing the big picture. I thus concur with PCAOB Board Member Steve Harris's comment that "the proposal would not provide as much useful information for investors as he had hoped". The point is not about those matters that are addressed by the audit of the financial statements but about those issues that are not being addressed per my commentaries of above. In other words, you need to be thinking about all of the stakeholders in a company and not just the investors.

When Chairman James Doty's comments that "the proposed standards would make the audit report more relevant to investors by establishing criteria and a framework providing deeper insights from the audit, based on information the auditor already knows from the audit", I say, that this is quite miniscule and not worth the bother. Thinking about the range of miscues we have experienced over the past ten years and the modifications as represented by these proposed changes to the auditor's report, I believe these modifications would have made minimal difference to these previous events.

Below is a summary of some of the key deficiencies of both the COSO and COSO ERM frameworks.

In conclusion, your proposed releases will accomplish very little. While we recognize the good work being done by the PCAOB, we will continue to see disaster after disaster in the corporate world in the United States. What needs to change is the way the external auditors perform their audit. Instead of commencing from the financial statements, they need to work off of the risk management plan of the company including the strategic objectives and then filter this information down to the financial statements. This involves intensive coordination with several other groups in the company, including internal audit. This is a much different approach to risk assessment than that currently being deployed.

The approach I am describing is integrated in nature whereas the public accounting model is linear. Just as you made the switch from rules based thinking to principles based thinking, so too is the switch needed that I am describing.

I reference you as well to the Financial Reporting Council in the United Kingdom and their recently released draft at the following link http://frc.org.uk/Our-Work/Publications/FRC-Board/Consultation-Paper-Risk-Management,-Internal-Contr-File.pdf. You will note how they now wish to interpret the audit of the financial statements. I l also reference you to a case study just prepared with two other colleagues that is being published shortly by John Wiley & Sons, and this will provide useful information for you. This book will be part of a best in class book of case studies on enterprise risk management as a companion to the highly successful *Enterprise Risk Management: Today's Leading Research and Practices for Tomorrow's Executives* (Wiley: 2010). Finally, I reference you to HB 436 just released by Australia/New Zealand which is worthy of a gold medal in terms of how risk management should be implemented by a company and this encompasses the audit of the financial statements. This is a product of a working group under the Standards Australia and Standards New Zealand Joint Risk Management Committee. This is referenced at:

http://shop.standards.co.nz/catalog/436%3A2013%28SA%7CSNZ+HB%29/view or

http://infostore.saiglobal.com/store/Details.aspx?productID=1694350

Thank you for consideration of my comments.

Sincerely yours,

Arnold Schanfield

Appendix

Some of the Key Deficiencies in the COSO and COSO ERM frameworks

- COSO was originally issued in 1992 and was a rule based document until the new release in May 2013. So for a 21 year period, implementation of internal controls followed rules based thinking
- The COSO framework just released in May 2013 as did the framework of 1992 and the COSO ERM framework, only defines risk in the "downside". But where does the upside of risk get reflected? For example, where does the risk get captured if we fail to properly monitor competition which does not allow our company to capture their customers in the event say that our major competitor goes out of business?
- There is almost no reflection in any of these documents on the role of the stakeholder in a company but plenty of attention focused on a company's investors. This is a very narrow interpretation of internal control and to my example above of British Petroleum, what about the fishermen that lost their livelihoods, the contractors that lost their lives, the environmentalists, the many local businesses that went bankrupt
- There is no reflection in any of these document of the slow demographic shifts from around the globe that create risk for a company
- The principle based approach of COSO ERM feels like a bolt on at the back instead of being woven into the material throughout the document. There is no mention of principles until you reach back of the book and then are confronted with 120 principles. The majority of these principles sound like more rules than principles and in any event, there is not attempt to tie these principles back to the literature.
- There is no distinction in any of these documents and especially that of COSO ERM, as to the difference between the risk management process and the risk management framework. In fact the COSO ERM cube completely ignores the risk management framework in a company and hence subjects such as stakeholders, communication process, commitment and mandate by the board, risk management policy, and context are completely ignored.
- No attempt is made to provide a completely integrated example either in the internal control framework or in the enterprise risk management framework. What appears are numerous disjointed examples

- No attempt is made to identify what constitutes effective risk management. See HB 436 which does a splendid job of this
- The authors of these documents appear to comprise a broad array of individuals but at end of the day, this initiative ignored the key risk management practitioners from around the globe and especially the material that such practitioners previously issued
- The subject of risk appetite to a company is not well understood and certainly not communicated in a way that can allow a practitioner to implement this effectively in a company. The leading professionals are now opting to use risk criteria and we encourage you to follow up HB 436 as I had indicated above