December 5, 2012

Mr. David L. Landsittel
Chairman
Committee of Sponsoring Organizations of the Treadway Commission

c.c. Elisse Walter, Incoming Chair U.S. Securities & Exchange Commission
Sent by e-mail

Re: COSO Re-exposure Draft and Related Guidance Dated September 2012

Risk Oversight Inc. ("RO") is a specialized risk management consulting and technology company with offices in Calgary, Alberta and Oakville, Ontario, Canada. The author of this comment letter, Tim Leech Managing Director of Global Services at RO, has been working globally in the area of risk and control management and reliable financial reporting for over 25 years. We appreciate the opportunity to comment on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO)'s September 2012 re-exposure drafts and related guidance.

NOTE TO READERS: The focus of our response is on the use of the proposed September 2012 COSO framework and related guidance for forming opinions on the effectiveness of financial accounting controls. Based on our global field experience and research done by the Institute of Management Accountants in 2006[1] the adoption and tangible use of the COSO 1992 framework to assess the effectiveness of controls and other risk treatments in areas beyond financial reporting, such as product quality, customer service, regulatory compliance, safety, minimization of unnecessary costs, IT security, fraud prevention and detection has not been widespread.

[1] COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices, Parveen P. Gupta, Institute of Management Accountants, 2006.

POINTS RAISED BY RO AND OTHERS IN RESPONSE TO THE DECEMBER 2010 COSO EXPOSURE DRAFT

In RO's comment letter to COSO's December 2011 exposure draft[2] we raised a number of serious concerns with the accounting control standards setting role COSO has been assigned by the Securities Exchange Commission for purposes of Sarbanes-Oxley section 404. In that response we recommended that responsibility for development of global accounting control standards be reassigned to the International Federation of Accountants. The concerns we raised related to COSO's standard setting structure and due process have also been raised by a number of other respondents to the December 2011 COSO exposure draft, as well as respondents to the September 2012 re-exposure draft.[3] We can find no reference or recognition of this issue by COSO in the section of the re-exposure draft titled "Public Comment Letters" starting on page 161 of the re-exposure draft.

We believe that the comment from the Institute of Chartered Accountants and Wales[4] ("ICAEW") best summarizes the views of many detractors with respect to the COSO December 2011 exposure draft:

We are therefore disappointed that the proposed revisions to the ICIF document do not appear to reflect major developments in business risk and control over the last twenty years. The revised document can give an impression of the need to be seen to be doing something whilst not making changes that reflect the more significant, recent developments.

The ICAEW's comment letter raised particular concerns with the de facto role of COSO as a global accounting control standard setter:

---

[2] Risk Oversight/Tim Leech response to COSO December 2011 exposure draft, March 19, 2012, http://www.ic.coso.org/Lists/UploadedFiles/Attachments/43/f9bfa636-bffa-4abd-b014-ed27b64c75cc_Risk%20Oversight%20Response%20-%20COSO%2020%20year%20Update.pdf

[3] For examples see the American Bankers Association response at http://www.ic.coso.org/Lists/UploadedFiles2/Attachments/2/ABA%20Comment%20Letter%20on%20revised%20COSO%20Proposal%20on%20Internal%20Control%20Framework%2011-2012.pdf and concerns raised by International Federation of Accountants specific to COSO guidance on internal control over financial reporting http://www.ic.coso.org/Lists/UploadedFiles2/Attachments/12/International%20Federation%20of%20Accountants.pdf

[4] Institute of Chartered Accountants of England and Wales to COSO December 2011 exposure draft, April 5, 2012, http://www.ic.coso.org/Lists/UploadedFiles/Attachments/123/ICAEW%20response%20to%20COSO%20ICIF%20ED%20.pdf

2.6 Governance of COSO and due process

26. *ICAEW is a member body of FEE, the European Federation of Accountants. We support FEE's comments on the governance of COSO provided in the appendix to their comment letter to COSO dated 13 March 2012.*

27. *We hope that COSO will give full and careful consideration to all comments received on this and related matters from all respondents.*

28. *We assume COSO will provide substantive feedback on this, and all other significant issues raised by respondents, as part of the overall, due process for the ICIF document.*

The European Federation of Accountants Appendix comments referenced by the ICAEW in their response included the following observations:

In comparison with other international organisations that are charged with setting internationally applicable standards used worldwide, the development of a framework like the COSO Framework on internal control should be framed by a governance structure of the organisation that supports the public credibility of the framework. Furthermore, a governance structure should:

Effectively promote the organisation's mission of developing comprehensive frameworks and guidance in the global marketplace on enterprise risk management, internal control and fraud deterrence designed to improve organisational performance and governance and to reduce the extent of fraud in organisations.

Provide for a standard setting environment that is independent of vested interests, while still ensuring the appropriate accountability to its wide range of global stakeholders.

Therefore, the governance of the COSO organisation could be improved in for instance the following areas:

Broader diversity, including geographical representation and representation by user groups in the COSO Board. This would balance public interest considerations with the technical expertise needed in the development process of the framework which will also strengthen the global political and technical accountability of the framework.

Improving the transparency of the appointment process of board members, including setting uniform appointment criteria for board members, such as through a body with supervising responsibilities that includes a nomination committee. In particular, the nomination committee should ensure that board members are appointed from a sufficiently large pool of candidates.

Ensuring a sustainable funding of the activities.

Ensuring that the development of the framework is done in a transparent way that is independent of vested interests. [5]

In light of the fact that that U.S. Congress decided to strip the AICPA of the auditing standards role it maintained for decades and assign responsibility for auditing standard setting to the PCAOB when they enacted the Sarbanes-Oxley Act over ten years ago, we are surprised that the SEC has continued to endorse the dated 1992 COSO internal control integrated framework as a "suitable" accounting control standard, and PwC, a "big four" auditing firm, as principal pro-bono author of the 1992 COSO standard and proposed 2013 standard. We believe the onus is on COSO to explicitly indicate to the SEC that it is not currently properly constituted, financed, or equipped to fulfill the role of global accounting control standard setting.

USE OF A CONTROL CRITERIA CENTRIC FRAMEWORK TO FORM BINARY OPINIONS ON CONTROL EFFECTIVENESS

To date the SEC has resisted calls to reconsider its decision to designate the dated 1992 COSO internal control integrated framework and the similarly dated 1994 UK Cadbury framework and 1995 Canadian CoCo control frameworks as "suitable" standards for public company reporting on internal control effectiveness.[6] We believe that it is highly likely, in the absence of a significant and immediate SEC direction change, that the COSO 2012 re-exposure draft is the most likely candidate to become the new SEC endorsed de facto global accounting control assessment, auditing, and reporting standard.

---

[5] European Federation of Accountants COSO exposure draft comment letter, March 13, 2012, http://www.ic.coso.org/Lists/UploadedFiles/Attachments/34/bcbfc8cd-d903-44ab-8ad0-c56378535291_COSO%20Internal%20Control%20Integrated%20Framework%20120313.pdf

[6] See COSO: Is "it" Fit For Purpose?, in Governance, Risk and Compliance Handbook, (Hoboken, NJ, John Wiley & Sons, Inc. 2008)

We do not believe that this would be in the best interest of the SEC or users of public company financial statements around the world. By copy of this letter we are respectfully requesting the SEC reconsider their position on this important issue.

It is also important to note that COSO has explicitly rejected calls from multiple sources to the December 2011 exposure draft to integrate the internal control framework with the COSO 2004 ERM framework[7]. The September 2012 COSO re-exposure draft confirms that COSO continues to promote and support the use of what we refer to as a "control criteria-centric" approach to evaluating and reporting on internal accounting control effectiveness, including its use for reporting on effectiveness of accounting controls. The control criteria-centric approach requires users form an opinion whether the company being assessed does, or does not, manifest the attributes of the control criteria being used. In the case of the COSO September 2012 re-exposure draft, the criteria are the 17 principles and hundreds of "Points of Focus" and "Approaches" delineated by COSO in the main Framework and supporting guidance.

We believe that the control criteria-centric approach to assessment of accounting controls which is often supplemented in practice for SOX 404 work with "process-centric" and "compliance-centric" methods is not optimal and is not in the best interests of stakeholders. Since the SEC mandated the use of COSO Internal Control Integrated Framework 1992 for reporting on accounting control effectiveness in 2004, CEOs, CFOs, and external auditors of tens of thousands of public companies have concluded that their accounting controls are effective in accordance with the criteria in the 1992 COSO internal control integrated framework and later been forced to restate their financial statements to correct material accounting errors.[8]

While we believe that the September 2012 re-exposure draft represents a significant improvement over the seriously dated 1992 internal control integrated control framework, we do not believe that a control criteria-centric approach is well positioned to minimize the frequency of materially unreliable auditor certified financial reporting. MF Global represents a recent high profile company where the CEO, CFO and PwC, its external auditor and primary author of the COSO September 2012 re-exposure draft, all certified that MF Global had effective accounting controls in accordance with the 1992 COSO Internal Control Integrated Framework. We believe that frequent incorrect opinions on the effectiveness of accounting control and reliability of financial statements using the control criteria-centric approach is

[7] COSO Internal Control Integrated Framework, Framework and Appendices, September 2012, page 164, paragraphs 580-582.

[8] For more information see Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act, Tim Leech and Lauren Leech, International Journal of Disclosure and Governance, September 2011.

something that should be expected by the SEC and users of financial statement because of its inherent weaknesses.

Since the 2008 global financial crisis there has been steadily increasing global recognition of the need for boards to effectively oversee management's risk appetite and tolerance. An area of particular board focus needs to be management's risk appetite and tolerance related to risks that threaten the reliability of a public company's financial disclosures. To highlight the importance of risk management the SEC introduced new disclosure requirements in 2010 requiring companies publicly disclose how a company's board oversees risk[9]. Similar public disclosure requirements were introduced in Canada.[10]

Unfortunately, the control criteria-centric approach to assessment of accounting control effectiveness provides subjective opinions on whether a company does or does not manifest the elements in the selected control criteria framework, not the level of retained risk of materially wrong financial disclosures. In the case of the COSO September 2012 re-exposure draft, it will be conformance to the 17 principles and hundreds of "points of focus" and "approaches". The control criteria centric approach provides very little information for senior management, boards of directors, or external auditors on the financial statement line items and notes with the highest levels of residual risk or, stated another way, the highest uncertainty the line items and notes are reliable.

We believe that stakeholders around the world would be better served by requiring companies use what we call an "objective-centric" approach to assessing risks to the macro objective of producing reliable/GAAP compliant financial disclosures, and the supporting sub-objectives of reliable financial statement line item and note disclosures. The core elements of the assessment approach we advocate are drawn from ISO 31000: 2009, the global risk management standard supplemented by best available risk treatment guidance.

Details on the assessment approach we believe would produce the information necessary for boards and external auditors to evaluate the residual risks being accepted that could lead to materially wrong financial disclosures is included in a discussion paper co-authored by Tim Leech and Jeffrey Thomson, CEO of the Institute of Management Accountants. The September 2006 discussion paper is titled "A Global Perspective On Assessing Internal Control Over

[9] Proxy Disclosure Enhancements, Release no. 33-9089, SEC (www.sec.gov/rules/final/2009/33-9089.pdf).
[10] McCarthy Tetrault, "CSA Provides Guidance on Corporate Governance Disclosures," March 2011 (www.mccarthy.ca/article_detail.aspx?id=5304).

Financial Reporting"[11]. The COSO 2013 framework could serve as one of the risk treatment reference guides referenced in this paper, in addition to globally acknowledged frameworks that have undergone significant development due process like the ISACA COBIT framework for IT security risk treatments, the OCEG GRC Maturity Framework, RO RiskStatusOversight™ risk treatment design principles, and others. Additional details on the advantages of an objective-centric approach to assessing the effectiveness accounting controls/risk treatments can be found in the December 6, 2012 Conference Board Director Notes publication "Board Oversight of Management's Risk Appetite and Tolerance.[12]

In summary, we sincerely and respectfully request COSO and the SEC seriously reconsider our 2011 recommendation to transfer responsibility for developing accounting control assessment standards to the International Federation of Accountants. In the likely event our recommendation is rejected, we sincerely and respectfully request COSO reconsider its decision to endorse and promote the use of "control criteria-centric" approach for purposes of assessing the effectiveness of financial accounting control. We do not believe it is the best approach available today to reduce the high frequency of materially wrong financial statements.

Yours sincerely,

Tim J. Leech FCPA CIA CRMA CFE

Managing Director Global Services

[11] A Global Perspective On Assessing Internal Control Over Financial Reporting, Tim J. Leech, Jeffrey Thomson, Institute of Management Accountants discussion paper, September 2006 , http://www.leechgrc.com/pdf/kb-sps/A%20Global%20Perspective%20on%20Assessing%20IC.pdf

[12] Board Oversight of Management's Risk Appetite and Tolerance, Tim J. Leech, Conference Board Director Notes Series, December 6, 2012.