risk oversight
A better response to risk.

January 13, 2014

TO: Financial Stability Board

Re: Request for Comments on "Increasing the Intensity and Effectiveness of Supervision: Consultative Document Guidance on Supervisory Interaction with Financial Institutions on Risk Culture" 18 November 2013

Risk Oversight Inc. ("RO") is a specialized risk management training, consulting, and technology company with offices in Calgary, Alberta and Oakville, Ontario, Canada. The primary author of this comment letter, Tim Leech, Managing Director Global Services, has been working in the areas of board risk oversight, internal audit, ERM, and reliable financial reporting for over 25 years, including work for major financial institutions globally. We have monitored FSB's initiatives closely and applaud the excellent work being done to improve the stability and soundness of the world's highly inter-connected financial systems.

While we believe that directionally FSB's guidance to regulators around the world has been outstanding and much needed, we don't believe it has identified a fundamental regulatory problem – regulatory reinforcement of management, board, and internal and external audit practices and paradigms that do not support, even conflict with, the type of effective risk appetite framework and risk culture being promoted by FSB. This response describes what we believe are regulatory reinforced handicaps to better, more effective and efficient risk oversight and management. At a summary level these include:

1. Regulatory imposed binary reporting from management, boards and external auditors on internal control "effectiveness" related to financial reporting and other topics.

2. Regulatory support for internal audit approaches that provide spot-in-time, subjective opinions on internal control effectiveness, but not reliable information for boards on management's risk appetite and tolerance.

3. Regulatory support for the practice of creating and maintaining "Risk Registers".

4. Reluctance on the part of regulators to investigate and identify root causes why traditional approaches to ERM and internal audit have failed in colossal ways in thousands of cases.

216 CARLINI COURT, SUITE 201, OAKVILLE, ONTARIO, CANADA, L6K3Y8 | (M) 416.720.0392 | ()) 905.339.2606

www.riskoversight.ca

POINT 1 - Regulatory imposed binary reporting from CEOs, CFOs, and external auditors on internal control "effectiveness" related to financial reporting and other topics

Following the enactment of the Sarbanes-Oxley Act in the U.S. in 2002, the SEC and PCAOB implemented requirements forcing CEOs, CFOs and external auditors to form opinions and publicly report on whether the company did, or did not, have "effective" internal controls over financial reporting against the dated 1992 COSO internal control integrated framework. SEC and PCAOB rules require that the opinions from management and external auditors on control effectiveness be binary. Regulators in Canada and elsewhere around the globe directionally followed the U.S. lead. The UK specifically rejected this approach. Since many of the world's largest companies and financial institutions maintain listings on U.S. security exchanges, the impact of this decision continues to have a profound impact globally. It is important to note that virtually all of the financial institutions at the root of the 2008 global financial crisis were judged to have "effective" internal control systems in accordance with 1992 COSO control framework by their CEOs, CFOs, and external auditors. No research has been undertaken that we are aware of to better understand why literally thousands of opinions on control effectiveness were colossally wrong.

In spite of tens of thousands of billion dollar plus failures of this assurance approach since it was introduced in 2003, no changes have been implemented. Binary opinions on control effectiveness are still required from CEOs, CFOs and, and external auditors in the U.S. and elsewhere around the world by regulators. What is not appreciated is that these requirements have retarded the development of effective risk appetite frameworks by not focusing resources on the task of ensuring boards of directors and external auditors are fully apprised of the line items in balance sheets and income statements and important note disclosures with the highest composite uncertainty/retained risk, and the potential impacts of that uncertainty. It isn't feasible to describe in a brief letter the full ramifications and negative impacts on effective risk management and risk appetite frameworks of this U.S. decision. We encourage the FSB to review the much lengthier and detailed analysis contained in an article by the author of this letter and his daughter titled "Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act[1]. This paper was sent to the SEC, PCAOB and U.S. Congress and received global exposure but no response.

[1] Tim Leech, Lauren Leech Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act, International Journal of Disclosure and Governance, Macmillan Publishers, 2011.

It is our belief that the SEC decision to continue to require binary reporting on control effectiveness over financial reporting significantly handicaps efforts globally to promote and foster more effective risk appetite frameworks.

Additional details on why the practice of requiring internal or external auditors to form subjective opinions on whether they believe controls are "effective" is handicapping effective board risk oversight can be found in a very recent article published by Conference Board Director Notes authored Parveen Gupta and Tim Leech titled "Risk Oversight: Evolving Expectations for Boards"[2]. FSB guidance on effective risk appetite frameworks is featured prominently in this article.

POINT 2 - Regulatory support for internal audit approaches that provide spot-in-time subjective opinions on internal control effectiveness, but not reliable information for boards on management's risk appetite and tolerance

Regulators have for the most part, been very supportive of companies creating and maintaining internal audit departments. Based on our observations and work with hundreds of internal audit functions globally, the effectiveness of these functions varies enormously. Many regulators have increased efforts to review and assess the competency, independence and professionalism of these functions and are now starting to call on boards of directors to spend more time assessing effectiveness of their internal audit functions. Unfortunately, what most regulators have also continued to encourage is proliferation of internal audit practices that discourage true management ownership and accountability for assessing and reporting upwards to boards on the true state of residual/retained risk.

In the majority of large financial institutions the internal audit departments create and maintain "risk-based" internal audit universes, complete spot-in-time assessments on a relatively tiny percentage of the assurance universe, and report whether internal audit believes internal controls are effective and, what are often called, "control deficiencies" or "control findings". These methods do not, in a material way, foster management ownership of risk management or produce reliable composite information for senior management and boards on the current residual risk status related to the achievement of key objectives. It is ironic that the central internal audit paradigm of direct report auditing (where internal audit is primary risk/control analyst/reporters) actually discourages true management ownership of risk assessment and reporting. While we recognize that the 2013 FSB guidance has called on internal audit to report on effectiveness of risk appetite frameworks, it has not recognized the debilitating impact of

[2] Parveen Gupta, Tim Leech, Risk Oversight: Evolving Expectations for Boards, The Conference Board Director Notes, January 2014.

regulators continuing to support the traditional internal audit paradigm. Research conducted by the IIA suggests that very few internal audit departments are dedicated any significant percentage of their time to formally assessing and reporting on the effectiveness of their company's risk appetite frameworks, or fostering true management ownership of risk management and reporting.

POINT 3- Regulatory support for the practice of creating and maintaining "Risk Registers".

Some years ago the UK updated what was then called the "UK Combined Code". It is now referenced as the UK Corporate Governance Code. One of the requirements was that companies should implement frameworks to better identify and assess risks. Unfortunately, for a variety of reasons, including advice from many of the world's largest and most influential audit and consultancy firms, this was interpreted to mean creating a maintaining what is generally referred to as "risk registers" or "risk lists". ERM has been interpreted by a large percentage of companies globally to mean a perfunctory annual or semi-annual update of these risk registers. This interpretation was driven, at least in part, by inferences in the 2004 COSO ERM framework and other authoritative guidance and papers that the primary way to implement ERM was to create and maintain risk registers and develop and communicate heat maps and risk lists of top 10, 20 or 100 risks for boards to review. This has caused boards, companies and auditors to come to see the practice of creating and maintaining these risk registers to be a regulatory requirement, not an effective way to manage and monitor management's risk appetite and tolerance and run a sustainable and successful business.

Full technical details on the unintended negative consequences of regulators encouraging broader use of risk registers and other "risk-centric" forms of assurance are described in a Risk Oversight white paper titled "The High Cost of ERM HERD MENTATITY" and THE CONFERENCE BOARD DIRECTOR NOTES Gupta/Leech January 2014 paper "Risk Oversight: Evolving Expectations for Boards" referenced earlier.

POINT 4 - Reluctance on the part of regulators to investigate and identify root causes why traditional approaches to ERM and internal audit have failed in colossal ways in thousands of cases

Following the 2008 global financial crisis the Senior Supervisors Group undertook ground breaking work to identify root causes. Although this work produced incredibly important insights and recommendations, we don't believe it dug deep enough or spend sufficient resources to understand why the ERM and operational risk management frameworks, internal

audit processes, and board risk oversight frameworks in the institutions at the root of the crisis failed.

Research completed by the Finance GRC Research Center at the Institute of Management Accountants in the U.S. titled "Accounting Control Assessment Standards: The Missing Piece in the Restatement Puzzle[3] did some very limited, small scope analysis on the issue and proposed a number of significant changes. Unfortunately, at the current time, few regulatory resources are being spent to research in a systematic way the root causes that explain why boards, senior management, and external auditors continue to issue materially wrong financial disclosures to investors, lenders, regulators, and other key stakeholders at a rate viewed by most of those impacted by those unreliable disclosures as grossly unacceptable.

We believe that one of those root causes for the lack of real change is a continued emotional attachment globally by regulators and the internal and external audit professions to promoting and relying on subjective control effectiveness statements from CEOs, CFOs, internal and external auditors. What we have recommended in numerous papers and presentations is that the focus and the massive resources being spent to generate these often unreliable internal control effectiveness representations be redirected to producing reliable information on the state of residual/retained risk for boards and external auditors. We find the continued support by regulators for subjective audit and management opinions on control effectiveness surprising since we be believe that it is actually severely handicapping efforts to encourage companies to develop, implement, and maintain more effective risk appetite frameworks.

We sincerely hope FSB finds our comments helpful. We would be happy to meet in person and answer any questions and further elaborate on the points made in this brief comment letter.

Yours sincerely,

Tim J. Leech FCPA CIA CRMA CFE

Managing Director Global Services

[3] Institute of Management Accountants Finance GRC Research Practice: The Missing Piece in the Restatement Puzzle, February 2008.