ro risk oversight
A better response to risk.

January 14, 2013

Catherine Woods
Financial Reporting Council
Fifth Floor
Aldwych House
71-91 Aldwych
London WC2B 4HN

Sent by e-mail

Re: FRC Consultation Draft: Risk Management, Internal Control and the Going Concern Basis of Accounting November 2013 Request for Comments

Tim Leech, the author of this comment letter, has been working globally in the area of risk and control management and reliable financial reporting for over 25 years. He has provided input and commentary on laws, regulations, and risk and governance related standards and guidance on multiple occasions; presented papers and proposals to the Securities Exchange Commission and Public Company Accounting Oversight Board in the United States and the Canadian Public Accountability Board in Canada; and presented scores of presentations and technical papers for the Institute of Internal Auditors ("IIA") globally, the ACCA in the UK, the CICA/CPA in Canada, the AICPA and Institute of Management Accountants in the U.S., the Institute of International Research globally, the U.S. and Canadian Conference Boards, and many others. We appreciate the opportunity to comment on the FRC November 2013 consultation draft.

Our first observation is that the FRC is to be congratulated for taking the lead globally in aggressively mandating enhanced board risk oversight for all publicly listed companies. The strategic direction of the November FRC consultation draft is consistent with recommendations of the Financial Stability Board in its July 2013 exposure draft "Principles for an Effective Risk Appetite Framework"; recommendations made by the National Association of Corporate Directors in the U.S. in their Blue Ribbon Commission Report "Risk Governance: Balancing Risk and Reward"; leading-edge guidance on risk governance and oversight issued by the ICGN to institutional investors; and others. Based on our analysis and monitoring of global risk and control governance standards over the past 30 years, we believe this guidance has the potential to position the UK and the London Stock Exchange as global leaders fostering enhanced risk governance in public companies.

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

Having dealt with what is sometimes termed, the "half full congratulatory perspective", we would like to respectfully offer a number of recommendations that may be perceived as harsh and radical by some, or more generally as the "half empty critical perspective". These suggestions are offered in good faith with the sincere hope they will make a meaningful contribution to preventing yet another wave of wide-spread, crippling corporate governance failures, while still encouraging and allowing businesses to take the risks they must to drive national prosperity and increase shareholder value.

In addition to the comments in this letter, we have also attached for your information a comment letter we filed today with the Financial Stability Board ("FSB") in response to their November 2013 consultative draft titled "Increasing the Intensity and Effectiveness of Supervision: Guidance on Supervisory Interaction with Financial Institutions on Risk Culture 18 November 2013". It contains our analysis of areas where we believe regulators in countries around the world have unintentionally created handicaps to better risk governance.

To keep this letter short, we are providing highly summarized recommendations while referencing additional technical support via links to relevant developments, technical papers, and research.

Recommendation #1 – Retitle the guidance "Risk Governance and Oversight Guidance".

The opening section of the guidance references the need and desire to transition from traditional "internal control" centric guidance to a new emphasis we think is best capsulized as "Risk Governance and Oversight Guidance". The words "internal control" in the title should be dropped and the issue of the going concern basis of accounting dealt with via areas of particular focus mandated in the paper.

Research done by the Institute of Management Accountants in the U.S. and Tim Leech, author of this paper, support the view that multiple waves of regulatory intervention since the 1970s, most recently mandating massively expensive compliance exercises, with a focus on forcing CEOs, CFOs, boards of directors, and external auditors to publicly represent that they have "effective internal control", have been ineffective at best, potentially perceived, less charitably, as spending a lot and accomplishing little.

In the period following the major governance breakdowns in the early 1980s, led by companies like Enron, HealthSouth, Parmalat, and many others, the U.S. enacted the Sarbanes-Oxley Act of 2001 including the now infamous, section 404. Section 404 requires annual representations by CEOs, CFOs and external auditors that controls are effective in accordance with the dated and,

in our opinion, technically flawed, COSO Internal Control Integrated Framework. In 2006 IMA research identified the fact that CEOs and CFOs of 1 in every 8 public large companies in the U.S. and their external auditors represented that their controls were "effective", in accordance with COSO 1992, and capable of preventing even a single material error. The need to subsequently restate their accounts suggests this strategy was sub-optimal at best, in spite of the massive multi-billion dollar costs globally. More recently, virtually all companies at the root of the 2008 global financial crisis and their external auditors publicly represented that those companies had effective internal controls in accordance with the COSO 1992 integrated control framework prior to the 2008 financial crisis emerging. No documented research has ever been conducted that we are aware of to identify the failings in the methods used by scores of companies at the root of the 2008 crisis to conclude their internal controls were "effective".

Forcing yet more representations and board focus on the question of whether internal controls are "effective", while at the same time attempting to foster better risk management, using tools that have amply proven ill-equipped for the task, should be avoided. Doing away with references to "internal controls" in this guidance and replacing it with more contemporary terms including "risk treatments", "risk mitigation strategies" and a focus on senior management and the board identifying and understanding the true state of retained/residual risk would be a good start. Unfortunately, at this point, it appears that the U.S., Canada and other countries are ignoring the old adage "doing more of what you have always done will produce more of what you have always got" by continuing to mandate annual internal control effectiveness representations from all public companies.

Supporting Technical References:

Accounting Control Assessment Standards: The Missing Piece in the Restatement Puzzle, Institute of Management Accountants Discussion Paper, February 2008.

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, July 2011.

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

Recommendation #2 – Drop the assumption that creating and maintaining "risk registers/risk lists" constitutes effective risk management and promote "objective-centric" risk assessment

At different points throughout the paper there are statements that suggest that the authors believe a primary element of an effective risk framework should be to create and maintain yet

more registers/lists of top risks. This regulatory strategy, like the one above requiring representations internal controls are effective, has had a dismal track record at actually helping boards of directors better oversee management's risk appetite and tolerance, and external auditors arrive at correct opinions on the reliability of the accounts.

The primary goal of effective risk management frameworks should be to increase certainty objectives will be achieved while operating with an acceptable level of retained/residual risk. Promoting even greater use of risk registers/risk lists that: largely divorce risks from the specific objectives they relate; assume risks can be analyzed one by one in isolation of each other; are developed primarily using very time limited, often annual perfunctory "brain storming" as a primary technique; rarely are linkable in any direct, obvious way to the company's top objectives, or even objectives statistically proven as having potential to significantly erode value; and are rarely used as a core tool to better manage human resources and allocate capital need to discouraged, not encouraged and mandated, by national regulators.

Mandating even wider-spread use and adoption of risk registers/risk lists should be considered to also represent a strategy that fits the caption "doing more of what you have always done will produce more of what you have always got". It is highly likely, almost certain, that the majority of the companies at the root of the 2008 global crisis maintained risk registers/risk lists. We are not aware of any research having been undertaken to understand why these "risk registers/risk lists" have often missed identifying and assessing risks that have shaken the entire world's financial systems and resulted in the demise/nationalization of major financial institutions.

Supporting Technical References:

Risk Oversight: Evolving Expectations for Boards, Parveen Gupta and Tim Leech, Conference Board U.S. Director Notes, January 2014.
The High Cost of ERM Herd Mentality, Tim Leech, Risk Oversight White Paper, March 2012.

Recommendation #3: Do Not Dismiss Internal Audit functions as irrelevant

Although the draft guidance calls for boards to satisfy themselves that the companies they oversee have risk governance frameworks capable of supporting the high expectations outlined in the consultation paper, our observation is that few boards in the world are currently technically equipped to make that assessment themselves. In our opinion, asking external auditors for an opinion on the effectiveness of the risk management systems that produce the financial statements they must opine on would represent a serious conflict of interest. We believe that the recommendation proposed by the Financial Stability Board on page 10 in their July 2013 paper on effective risk appetite frameworks represents the best solution.

4.6 Internal audit (or other independent assessor) should:

a) routinely include assessments of the RAF on a firm-wide basis as well as on an individual business line and legal entity basis;

b) identify whether breaches in risk limits are being appropriately identified, escalated and reported, and report on the implementation of the RAF to the board and senior management as appropriate;

c) independently assess at least annually the design and effectiveness of the RAF and its alignment with supervisory expectations;

d) assess the effectiveness of the implementation of the RAF, including linkage to strategic and business planning, compensation, and decision-making processes;

e) validate the design and effectiveness of risk measurement techniques and MIS
used to monitor the firm's risk profile in relation to its risk appetite;

f) report any deficiencies in the RAF and on alignment (or otherwise) of risk appetite and risk profile with risk culture to the board and senior management in a timely manner; and

g) evaluate the need to supplement its own independent assessment with expertise from third parties to provide a comprehensive independent view of the effectiveness of the RAF.

While we believe the internal audit profession globally and in the UK must take immediate and radical steps to equip IIA members to meet these expectations, we also believe that requiring internal audit opine regularly on the effectiveness of the entity's risk appetite framework is the optimal risk governance strategy. Boards of companies that have elected not to have an internal audit function should obtain an opinion from other technically qualified and independent sources.

Supporting Technical References:

Thematic Review on Risk Governance Frameworks: Peer Review, Financial Stability Board, 12 Feb 2013.

Principles for an Effective Risk Appetite Framework, Financial Stability Board, 17 July 2013

Recommendation #4 – Delete all references to "internal controls" replace with "Risk Treatments", "Risk Mitigation strategies", and other globally accepted risk management taxonomy

Aligned with our Recommendation #1 above, we recommend that the guidance be re-written to use the globally accepted ISO 31000 risk management standard/ISO Guide 73 terminology. This means that segments of the guidance like the one used as an illustration below need to be replaced with the suggested wording.

Current wording: "Once those risks have been identified, the board should agree how they will be managed and mitigated, and keep the company's risk profile under review. It should satisfy itself that management's systems include appropriate controls, and that it has adequate sources of assurance;" (page 2)

Suggested wording: Once those risks have been identified, the board should agree how they will be managed and treated, and keep the company's risk profile under review. It should satisfy itself that management's systems include appropriate risk treatments, including appropriate choice of risk mitigation, risk share, risk transfer, risk financing strategies, and that it has adequate sources of assurance;

There are many instances in the November 2013 consultation paper where it uses older more traditional "control speak" language rather than using this paper as an opportunity to promote and foster more contemporary and technically correct risk management taxonomy. We believe the guidance in its current form has great potential to confuse and impede companies that are making diligent attempts to adopt better, more effective risk appetite frameworks by randomly mixing traditional "internal control" terminology with more contemporary risk management terminology. ISO Guide 73 was specifically developed to assist regulators globally when drafting regulation related to risk management. We don't believe that ISO's goal to promote global consistency in risk management taxonomy should be ignored by the FRC; and we don't believe the FRC should promote an approach that encourages one taxonomy for managing risks related to reliable accounting representations, and another quite different approach for the rest of the risks facing the enterprise.

Supporting Technical References:

ISO 31000:2009 Risk Management Principles and Guidelines, ISO

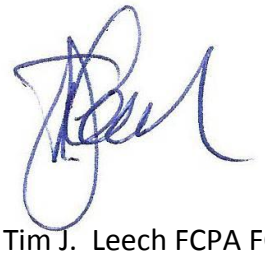
ISO Guide 73:2009 Risk Management Vocabulary, ISO

Honourably Retire "Internal Control" Promote "Risk Treatments": It's Time, presentation by Tim Leech at the October 2013 IIA All Star Conference, New Orleans, October 2013.

Concluding Remarks:

Many years ago my grandfather, who was a wise and experienced fishing guide in Canada, taught me a valuable lesson. He told me that if you are trying to board a boat that is not tied to the dock and the wind is blowing you need to make a decision. Are you going to get on the boat or get back on the dock and wait for another chance to get where you want to go. We believe that it has been very clear for some time there is an urgent need to look for a new and radically better corporate risk governance boat to board. It is well past time to retire the internal control effectiveness paradigm in favour of a new paradigm that relies on management, boards of directors, and external auditors demanding, and receiving, better information on the true state of retained/residual risk so they can better discharge their respective duties.

Yours sincerely,



Tim J. Leech FCPA FCA CIA CRMA CFE

Managing Director Global Services

ro 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.