risk oversight solutions
A better response to risk.

October 8, 2015

Mr. Mark Zelmer
Deputy Superintendent
Office of the Superintendent of Financial Institutions Canada
255 Albert Street
Ottawa, Canada
K1A 0H2

RE: Invitation to Comment E-21 Operational Risk Management Exposure Draft August 2015: RECOMMENDATION: REPLACE "THREE LINES OF DEFENCE" WITH "FIVE LINES OF ASSURANCE"

Dear Mr. Zelmer

Thank you for the opportunity to comment on OSFI's August 2015 exposure draft (ED) "Operational Risk Management". In light of the financial crisis of 2008, subsequent multi-billion dollar scandals related to LIBOR and FOREX, and the current dynamic and volatile economy the importance of this area, and the need for national regulators around the globe to "get it right", continues to build.

Credentials that support the views expressed in this comment letter span over 25 years of global experience working with financial service companies around the world helping them design and implement more effective enterprise risk management systems. A list of financial sector clients in the sector I have provided services to can be accessed at http://riskoversightsolutions.com/about-us/sample-clients/by-sector. A short summary of experience is located at http://riskoversightsolutions.com/about-us/ro-professionals/profiles/tim-j-leech.

The exposure draft covers a fairly broad range of expectations which are relevant and valuable. There are a number of areas of the ED that I think are particularly good and break new ground. My comments in this letter are limited to Section 4 Principle 3 shown below:

4. Three Lines of Defence
Principle 3: FRFIs ensure effective accountability for operational risk management. A 'three lines of defence' approach, or appropriately robust structure, serves to separate the key practices of operational risk management and provide adequate independent overview and challenge. How this is operationalized in practice in terms of the organisational structure of a FRFI will depend on its business model and risk profile.

I respectfully request that OSFI consider revising the draft guidance and replace the "THREE LINES OF DEFENCE" with what I reference as the "FIVE LINES OF ASSURANCE" framework.

The business case in support of this recommendation follows.

FRAMEWORK NOMENCLATURE - Contemporary risk governance professionals around the world promote the view that risk management and risk governance is fundamentally about increasing certainty that key objectives will be achieved while still operating within acceptable levels of residual risk. This interpretation flows from the ISO 31000 risk management standard definition of the word "risk" – the effect of uncertainty of achieving objectives. Using the ISO definition of risk objectives covered should include an organization's key value creation/strategic objectives, as well as objectives which have potential to significantly erode value.

I believe that the word "DEFENCE" used in the framework promoted in the OSFI ED connotes a heavy emphasis on hazard avoidance, a stigma attached to the discipline of risk management that many risk professionals are trying to change. In the sporting world teams that only practice defence as opposed to a balance of offence and defence won't score many goals and win games. A key role of risk management is to help senior management and boards decide on appropriate balance of resources between creating value and driving profits and complying with applicable laws and regulations to create wealth, drive national and international prosperity, and stay within social norms of acceptable conduct. Unfortunately, surveys indicate that boards of directors have been slow to apply formal risk management methods to strategic planning processes as they don't see the connection. One can argue that the 2008 financial crisis is rooted in flawed strategy adopted by a large number of significant financial firms. While I recognize that laws and regulations in the financial sector are heavily skewed to protecting the international and national economies as well as a range of stakeholders impacted by activities of financial institutions, I believe that national regulators also have a role to play promoting value creation and enhancing the wealth and well-being of national economies. This is best achieved by requiring and promoting the use of frameworks that promote a careful balancing of value creation and value protection.

TECHNICAL SUPPORT FOR FIVE LINES OF ASSURANCE – Not long after efforts began to elevate the THREE LINES OF DEFENCE approach, an approach coined and promoted by the Institute of Internal Auditors in 2013 and others earlier (see https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf) Protiviti, an international consulting firm, and others have, in essence, suggested that the THREE LINES OF DEFENCE model is incomplete and suboptimal at best, conceptually flawed at worst. A simple Google search on the term FIVE LINES OF DEFENCE quickly points to some of this debate and the key differences between the THREE LINES OF DEFENCE and what has been coined the FIVE LINES OF DEFENCE. The main difference in the FIVE LINES OF DEFENCE proposals are the addition of key roles identified for senior management and the board of directors. A link to a short bulletin published by Protiviti that describes the key elements of what they reference as FIVE LINES OF DEFENCE can be found at http://www.protiviti.ca/en-US/Documents/Newsletters/Bulletin/The-Bulletin-Vol-5-Issue-4-Applying-5-Lines-Defense-Managing-Risk-Protiviti.pdf. Given the huge importance of the role played by the C-Suite and board of directors in an effective risk governance framework, it would seem to make sense that regulators use every possible opportunity to elevate the risk governance roles and responsibilities of those two groups.

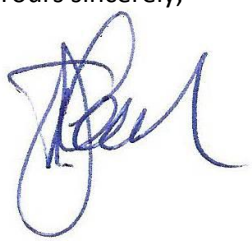
FINANCIAL STABILITY BOARD SUPPORT FOR FIVE LINES OF DEFENCE/ASSURANCE – As OSFI is no doubt very well aware as a result of active participation of OSFI staff, current and past, and the role of Mark Carney past Governor of Bank of Canada, current Governor Bank of England, and Chair of Financial Stability Board (FSB), the FSB has published a number of truly ground-breaking papers describing the

changes FSB believes national regulators should make to prevent a reoccurrence of the 2008 global financial crisis. One of those papers is the seminal November 2013 ***Principals for An Effective Risk Appetite Framework.*** (http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf) Pages 8 and 9 of that document do a great job articulating the risk governance roles that should be played by Chief Executive Officers and the Board of Directors. My analysis of the work of the FSB since it was constituted is that the FSB is, in fact, promoting a five line of assurance framework as key to achieving optimal results and preventing future financial crisis and global instability.

FIVE LINES OF ASSURANCE: The core elements of the FIVE LINES OF ASSURANCE approach we are promoting are described in the June Conference Board Director Notes paper "The Next Frontier: Board Oversight of Risk Culture" starting on page 6 under the heading "Board & C-Suite Driven/Objective Centric ERM and Internal Audit". We selected the name used in that paper to emphasize the key roles played by C-level staff and the board. It is important to note that, in essence, the approach we advocate is fundamentally a FIVE LINES OF ASSURANCE approach. The Conference Board paper can be accessed at http://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk-Oversight-The-Next-Frontier-for-Board-Oversight-of-Risk-Culture-Tim-Leech-and-Parveen-Gupta.pdf. The paper includes a description of the role we envision for business units, specialist risk groups, internal audit, the C-Suite and boards. More details on this approach can be found in slides used for a training session presented to Chief Audit Executives at the 2015 IIA International Conference held in Vancouver at http://riskoversightsolutions.com/wp-content/uploads/2011/03/IIA-Intl-Conference-July-2015-Tim-Leech-Risk-Oversight-Solutions-Audit-Transformation-Strategies.pdf. A sample policy that describes at a very high level the roles of the FIVE LINES OF ASSURANCE – business units, specialist support groups, internal audit, C-Suite, and the board of directors is included as Appendix A to this letter.

In closing, I sincerely believe that the global economy and national economies will be better served if financial and securities regulators around the world promote the core elements of what has been described in this letter as FIVE LINES OF ASSURANCE approach to risk governance. I don't believe it would be difficult to revise the current OSFI exposure draft and replace the THREE LINES OF DEFENCE with FIVE LINES OF ASSURANCE. Canada could be the first country in the world to actively elevate and officially add the C-Suite and Board of Directors to the overall operational risk framework regulators promote. Given Canada's success navigating the 2008 global crisis, this would be in keeping with Canada's past success and current enviable reputation in the global financial community. I would be happy to meet and discuss in more detail any of the points raised in this proposal.

Yours sincerely,



Tim J. Leech

FCPA FCA CIA CRMA CCSA CFE

APPENDIX A: Sample Corporate Risk Management Policy

PURPOSE:

The purpose of this policy is to create, enhance and protect shareholder value by designing, implementing and maintaining an effective, structured, and enterprise-wide risk management approach. We believe that adopting this policy will result in both immediate and long-term benefits to all stakeholders, internal and external. Benefits foreseen are:

- Increase the likelihood of achieving the company's business objectives.
- Enhance XYZ's competitive advantage.
- Deal with market instability more effectively.
- Enable XYZ to better meet customers' expectations and contractual requirements.
- Establish a Board level mandate to implement an enterprise wide approach to risk management to meet emerging risk management and risk oversight expectations.
- Enhance shareholder and customer confidence.
- Respond to escalating institutional shareholder demands for effective risk management frameworks in companies they invest in.
- Meet emerging credit rating agency expectations related to risk management.

SCOPE

This policy applies to employees, officers and directors of each of XYZ Energy Services Corp. and its Subsidiaries. References in this policy to the Corporation mean XYZ Energy Services Corp. and its subsidiaries.

POLICY

1.1 Risk Management Principles

Risk management is a systematic, structured, transparent, inclusive, and timely way to manage uncertainty and create and protect shareholder value. It should be adaptive to XYZ's business needs and a dynamic process. It should evaluate risk/reward trade-offs within the organization's appetite for risk tolerance.

It is intended to be an integral part of all organizational processes, including strategic planning and decision making, and is based on best available, "fit for purpose" risk information. It is dynamic, iterative and facilitates continuous improvement of the organization.

2.1 Corporate Risk Assessment Methodology

The risk assessment methodology the Corporation has selected focuses on end result business objectives that the company must achieve to be successful over the longer term and drive shareholder value. The key goal is identification and consensus agreement on the acceptability of the company's residual risk position (residual risk status is a composite snapshot the helps decision makers and the board better understand the level of uncertainty that exists that business objectives will be achieved).The risk management methods and tools used by the Corporation are expected to evolve and mature over time with an overriding goal that the amount of formal risk assessment applied (as opposed to informal risk management which happens every day in every part of the Corporation) will be determined by carefully considering the costs and benefits of the additional information.

3.1 Risk Management Roles and Responsibilities

The **Board of Directors** is responsible for:

a. Approving and authorizing this policy.
b. Assessing whether the risk appetite and tolerance implicit in the Corporation's business model, strategy, and execution is appropriate.
c. Assessing whether the expected risks in the Corporation's strategic plan are commensurate with the expected rewards.
d. Evaluating whether management has implemented an effective and fit-for-purpose process to manage, monitor, mitigate and report on risk that is appropriate given the Corporation's size, growth aspirations, business model, and strategy.
e. Assessing whether the Corporation's risk management processes are capable of providing reliable information to the board on the residual risk status related to key objectives that are or could impact on the achievement of the Corporation's objectives, including significant risks to the Corporation's reputation.

The **CEO** is responsible for:

a. Appointing the members of the Corporation's Risk Oversight Committee.
b. Assessing whether the Corporation's current and expected risk status is appropriate given the Corporation's and board of directors' risk appetite and tolerance.
c. Ensuring that there are reliable processes in place to provide the board of directors with an annual report on the effectiveness of the Corporation's risk management processes, and a report on the Corporation's consolidated residual risk status, including any remediation actions underway to adjust the Corporation's retained risk position.

The **Risk Oversight Committee** is responsible for:

a. Determining where and when formal documented risk assessments should be completed recognizing that additional risk management rigour and formality should be cost/benefit justified.
b. Ensuring that business units are identifying and reliably reporting the material risks to the key objectives identified in their annual strategic plans.
c. Reviewing and assessing whether material risks being accepted across XYZ are consistent with the Corporation's risk appetite and tolerance.
d. Developing, implementing, and monitoring overall compliance with this policy.
e. Overseeing development, administration and periodic review of this policy for approval by the Board of Directors.
f. Reviewing and approving the annual external disclosures related to risk oversight processes required by Canadian security regulators.
g. Reporting periodically to the CEO and the Board on the Corporation's consolidated residual risk position.
h. Ensuring that an appropriate culture of risk-awareness exists throughout the organization

Business unit leaders are responsible for:

a. Managing risks to their business unit's business objectives within the Corporation's risk appetite/tolerance.
b. Identifying in their business unit's annual strategic plan the most significant internal risks and external risks that have the potential to impact on the business unit's key objectives together with their plans to address those risks.
c. Reporting to the Risk Management Support Services unit the current composite residual risk rating on key objectives identified in the business unit's strategic plan and other objectives that may have been assigned to them by the Risk Oversight Committee and/or the CEO.
d. Completing documented risk assessments when they believe the benefits of formal risk assessment exceed the costs, or when requested to by the CEO or Risk Oversight Committee.

Risk & Assurance Services unit is responsible for:

a. Providing risk assessment training, facilitation and assessment services to senior management and business units upon request.
b. Annually preparing a consolidated report on XYZ's most significant residual risks and related residual risk status, and a report on the current effectiveness and maturity of the Corporation's risk management processes for review by the Risk Oversight Committee, senior management, and the Corporation's board of directors.
c. Completing risk assessments of specific objectives that have not been formally assessed and reported on by business units when asked to by the Risk Oversight Committee, senior management, or the board of directors; or if the Risk Management Support Services team

leader believes that a formal risk assessment is warranted to provide a materially reliable risk status report to senior management and the board of directors.

d. Conducting independent quality assurance reviews on risk assessments completed by business units and providing feedback to enhance the quality and reliability of those assessments.

e. Participating in the drafting and review of the Corporation's annual disclosures in the Annual Information

NOTE: When a company is of sufficient size the role of the risk management group and internal audit are separated. The primary role of risk management group is to help implement and maintain the company's risk assessment and reporting process. The primary role of Internal Audit is to provide reports on the effectiveness of the company's risk management/risk appetite framework and reliability and completeness of the consolidated report on residual risk status provided by the CEO to the board of directors.