March 16, 2011

Ms. Gigi Dawe
Principal, Risk Oversight and Governance
National Practice Leader, Governance, Strategy and Risk Management
Canadian Institute of Chartered Accountants
277 Wellington St. West
Toronto, ON
M5V 3H2

Delivered via email to: gigi.dawe@cica.ca

Dear Ms. Dawe,

**Re: Invitation to Comment: A Framework for Board Oversight of Enterprise Risk**

Financial Executives International Canada (FEI Canada), on behalf of the Corporate Governance Sub-Committee of the Issues and Policy Advisory Committee, is pleased to respond to the CICA's Invitation to Comment on the exposure draft *A Framework for Board Oversight of Enterprise Risk.*

We have prepared our response in the form of answers to the two specific questions raised in the Invitation to Comment. Our answers are presented in the attachment to this letter.

Overall, we support the concepts in the proposed framework. However, we have some suggestions to improve the usability of the framework in its current form, both for boards of directors and senior business leaders.

Given our conversation concerning the CICA's wish to focus on the risk oversight provided by boards of both large and small organizations, as well as the CFO's risk oversight responsibilities within an organization, FEI Canada would be pleased to work with you on these initiatives.

Yours truly,

***Michael Conway, CA, ICD.D***
Chief Executive and National President

***Wayne Braun, CMA***
Chair, Corporate Governance & Internal Control Committee

Encl.

**Invitation to Comment: A Framework for Board Oversight of Enterprise Risk**
**Comments by FEI Canada**

The following comments are responses to the specific questions raised in the Invitation to Comment.

1. ***How would this framework be helpful to you in your oversight responsibility for risk in the organization for which you are involved?***

   We believe the framework is a useful first step in providing guidance on risk oversight. As mentioned in the document, the board first needs help in cementing each director's individual knowledge and understanding of risk, and we suggest more guidance be provided on the actual oversight role that the directors should fulfill. It then needs to be satisfied that there is a real mechanism, especially within the second and third elements in the CICA framework (Identify/Categorize Risks and Analyze Consequences), for sufficient scope of management risk consideration and judgment.

   One concern we have is that the framework seems to suggest that it is the role of the Board to drive the risk management effort, rather than rely on management to drive it and the Board to oversee it. As the document itself points out, according to McKinsey:

   > *"traditional governance models support the notion that boards cannot and should not be involved in day-to-day risk management, but that directors should through their risk oversight role, be able to satisfy themselves that effective risk management processes are in place and implemented"*.

   In fact, best practice would suggest that the number one responsibility of the Board is to put the right executive management team in place and, if done correctly, they should be able to rely on them to lead the risk management efforts for the organization, and then focus solely on risk oversight by actively challenging management's assumptions through asking them the critical questions and measuring management's responses.

   Further, the framework does not appear to be able to cope with different types of organizations. Is it the CICA's intention to have this framework serve as a generic framework for any type of organization? The framework does not appear to be suitable for all organizations in all sectors (i.e. while some of the tools suggested might be best practice, they might not be cost efficient for any organizations other than the largest public companies. As well, it would be difficult for a not-for-profit board to use this framework).

   The CICA should either specify that this framework has been developed for profit-oriented publicly accountable enterprises of a certain size or industry type, or ideally rework the framework so that it has broader applicability.

***2. What would help to make the framework more useful to you?***

We have several suggestions that we would like the CICA to consider, and have broken these out into general comments and detailed comments specific to each section of the framework.

***General framework comments***

We believe it would be useful for the CICA to include the genesis of this particular framework in its overview. This framework should also be broadened to be more applicable to include smaller organizations.

Although the framework can act as a good starting point for companies, particularly for those that have not done work in this area before, it will need to be adapted for each industry/organization to address specific risk areas that are critical to them. The framework needs to be more explicit in demonstrating this.

The framework should also more clearly define the role of the Board versus the role of management and how each would carry out their particular risk management responsibilities.

One aspect that should perhaps be given more emphasis within the framework is that when risks have materialized unexpectedly, it has often not been because of a lack of an ERM framework. The 'black swans' of recent history have tended to arise from poor judgment within organizations that were supposed to have had a proper risk process. Therefore, the Board should be satisfied that there are formal recurring judgment processes behind the framework for:

1) identifying, prioritizing, and mitigating all risk factors (not just the ones identified in the framework which may be incomplete to start with and may not recognize changing circumstances);

and

2) assessing how management is applying judgment to them.

Without this, the existence of a framework could still foster board complacency, and an adverse event may still take everyone by surprise with the Board taken to task after the fact.

***Specific comments, on a section by section basis:***

1. <u>Introduction</u>
    a. Directors should understand what a risk management framework is versus learning a new oversight framework. Instead of providing a new framework, why not take an existing framework and explain how the Board can fulfill their oversight responsibilities?
    b. At the very least, the framework should provide reference materials related to the different frameworks available (eg, COSO's Enterprise Risk Management Integrated Framework, and ISO 31000's Risk Management Standard).

2. <u>Critical Issues</u> (starting on p2)
    a. The questions asked on page 2 are very good and should be asked at the Board level.
    b. Page 3 notes the fact that the Board should assist in determining the appetite for risk for the corporation – however, nowhere else in the document is this addressed. In fact, the last point questions judgments around risk tolerance – is the author using the two terms interchangeably? Risk appetite and risk tolerance are areas that the Board needs to understand and agree with. It would therefore be extremely useful in giving Boards guidance on what each term means and how each should be set, or providing reference materials on where they can obtain more information.

c. The paragraph on page 3 on "Board organization and structure for addressing risk" is good. So are the questions raised on page 4 for each topic area. In fact, these pages (3-5) are probably the key items for this framework and could be limited to asking the questions and providing guidance for what Boards should know. It seems as though the actual framework strays away from these concepts to a certain degree.

3. Preparing to Implement the Framework (starting on p7)

   P8 regarding involvement by the board – risk oversight is a critical responsibility of the Board, and therefore must include thoughtful discussion and interaction, drawing on all of the board members capabilities. We completely agree with this statement, yet the actual framework appears to have the Board do more hands-on work than may be appropriate.

4. Establish Context (p13)
   a. This appears to be a cursory review only. There is no detail identifying how or where a Board can gain the appropriate information. For example, would it be through management presentations, strategic planning, or some other method? Also, key stakeholders should be included in context. ISO 31000 also has "establishing the context" contained within its framework, but with a different take on what establishing context means. Therefore, using this language might confuse those familiar with that framework.
   b. Limiting the context to current conditions seems unduly restrictive and suggests the items are complete when they may not be. There may well be major decisions pending or foreseeable that the Board should consider as a part of the context. This is especially important since the risks referred to in "Categorizing Risks" may not be all-inclusive.

5. Identify and Categorize Risks (starting on p15)
   a. In general, far more emphasis has been placed upon listing possible tools to assist boards oversee the risks than describing the risks in detail. It would be helpful, particularly for smaller organizations that may not have the resources of large public companies, to provide more description of and guidance on the risks themselves.
   b. "Too often this process focuses on external risks..." where natural disasters, competition and environmental issues are cited as examples. We would disagree with this statement. Although a reasonable job is performed by companies in identifying external risks, there are studies that show that most companies spend more time identifying their operational (internal) risks. We believe it would be more appropriate to state that most companies do not focus on their strategic external risks.
   c. There is a risk identification 'framework' shown on p.16. This doesn't appear to be so much a framework as it is a graphic of key risk categories with examples of sub-categories of risk included in the descriptions. To call it a framework is misleading. We agree with reputational risk being appropriately identified as the consequence of acts. Perhaps it should be referenced as an outcome and not specifically referred to as a risk category. Finally, the graphic's reference to "Leadership" risk should be referred to as "Organizational" risk to be consistent with the related definitions provided.

6. Strategic Risk (starting on p17)

   We believe that overall this is very well written and provides some excellent guidance for both Boards and management. The key concern that we have in this section is there is a lot of reference to engaging external consultants to perform many types of assurance related tasks (such as performing interviews and performing process audits). Consideration should be given to alternate means of gathering information, particularly for smaller organizations that may not be able to afford extensively engaging consultants.

7. Merger and Acquisition Risk (p 24)
    a. For consistency, M&A risk should either be shown separately on the 'risk identification framework' provided on page 16 or shown as a subset of strategic risk. That said, we believe the information in this section gives good guidance.

8. Financial Risk (p 28)
    On p30 there is another reference for Boards to 'periodically assess cash availability under various scenarios...' under the capital availability review. How? The document refers to a discussion in the Risk Tolerance section, but it isn't addressed to any satisfactory means. Should boards really be performing this, or is this a critical question that they should pose to management?

9. Organizational Risk (p 31)
    This section provides good guidance. One other change that might be considered to reinforce financial prudence and independence of the CFO role would be to have the CFO jointly report to both the CEO and the Audit Committee Chair, as is almost the case in practice in many organizations.

10. Operational Risk (p34)
    a. We would have expected to see HR, IT security, physical assets (like plant facilities and the like) included in this section. They seem to have been ignored yet are all key categories of operational risk for most organizations.
    b. The guidance in this section appears to be very specific to goods producing companies. A focus on some IT security and HR components would make it far more applicable to a broader range of organizations. For example, what are the risks a service organization should consider?

11. External Risk (p36)
    In reading the framework and in consideration of what external risks are made up of, we believe that external risks should not exist as a separate category but rather reside under the strategy section as the tools used should be those used in strategic planning to assess the external environment. The risks that fall out generally fit into the other categories. In addition, while page 36 identifies unanticipated risks, how can they actually be dealt with since "unknown-unknowns" (i.e., black swans if severity is high) can not be anticipated. The discussion suggests some tools but it is hardly convincing that this set of tools is necessary and sufficient.

12. Analyze Consequences (p 39)
    a. It would be useful to provide more guidelines and tools. For example, many organizations use a four-quadrant chart as a useful visual tool to plot the severity of risk impact against the probability of occurrence along the "high/low" continuum of an X-Y axis.
    b. The ranking for severity and likelihood need to be better explained – or at least referenced to an existing ERM framework like ISO.
    c. On the Heat Map, we believe that by only having low, moderate and high rankings for likelihood will lead to a lot of moderately ranked risks. 4 or 5 factors would work much better as it becomes much more difficult to sit on the fence.
    d. Giving a combined risk rating (significance x likelihood) helps to properly identify the top ranked risks – then discussions can be held to decide if they have indeed been ranked appropriately.

13. Analyze Interconnectiveness (p43)
    a. We agree that it makes sense to look at the risk heat map; however, the interconnectivity diagram is hard to follow.

b. The author should also consider linking strategic objectives to the key risks identified. The use of a matrix is a very efficient way of identifying where there are interconnectivities. A detailed example would also assist in this regard.

14. Re-analyze Consequences (p45)
    a. This step should likely be relocated into the interconnectivity step, with a reference back to the Analyze Consequences section if the process is intended to be the same.
    b. Compared to earlier sections of the framework, there is very little guidance provided in this section.

15. Prioritize (p47)
    a. We believe that by using a combined risk ranking, the exercise of prioritization would be straightforward.
    b. There is very little guidance provided in this section and no tools have been identified to assist Boards in understanding how to assess the prioritization of risks by management. How do we know if management has properly assessed and prioritized risks and incorporated them into decision making? What if the cost considerations are given greater weight than safety in construction activities (e.g. BP Gulf of Mexico disaster)? Perhaps the framework will come to life if a large egregious example such as BP is used to illustrate how that situation could have been avoided, or at least mitigated.

16. Assess Risk Tolerance (p 49)
    a. We believe that this area is one of the least understood areas in risk management yet one that the Board should be much more aware of. Therefore, a lot of attention should be given to this topic – even if just to define what risk tolerance is and how it can be set, and how this differs from risk appetite.
    b. Setting risk tolerance is management's responsibility; however, the Board has a direct role in setting risk appetite. This framework is silent on this fact including even the process on how to do it. There should be at least one page dedicated to each topic with guidance given to the Board.

17. Choose Response Strategy (p51)
    a. This section contains a fairly light discussion. It would be useful if information was provided to assist the reader more clearly understand what the mitigation strategies are (i.e. avoidance, prevention, reduction, segregation of exposures, contractual transfer for risk control, and risk financing for losses / insurance).
    b. The examples given, including how strategies can tie to risks, are useful for management but it is of particular use to helping Boards understand what can be done. We do have a concern that if this is expressed in an oversight framework, the Board might believe it should be setting the strategy versus ensuring that the strategy is adequate.

18. Monitor (p 54)
    a. This section provides a good overview of what should be done by the Board.
    b. We would suggest providing some more robust red flag indicators or perhaps reference to other material that the board could use (such as information in the Director Series – like the CICA's *Financial Aspects of Corporate Governance* document as an example).

**About FEI Canada** (www.feicanada.org)

Financial Executives International Canada (FEI Canada) is an all-industry professional association for senior financial executives. With eleven chapters across Canada and more than 2,000 members, FEI Canada provides professional development, thought leadership and advocacy services to its members.

The Issues and Policy Advisory Committee (IPAC) is one of two national advocacy committees of FEI Canada. IPAC is comprised of more than 50 senior financial executives representing a broad cross-section of the Canadian economy who have volunteered their time, experience and knowledge to consider and recommend action on a range of topics of interest to Canadian business and governmental agencies. The current composition of IPAC is formulated to address the following areas: corporate governance, capital markets, tax policy, pensions, internal controls, information technology and public sector accountability. In addition to advocacy, IPAC is devoted to improving the awareness and educational implications of the issues it addresses, and is focused on continually improving these areas.