Arnold H. Schanfield, CPA, CIA
Principal, Schanfield Risk Management Advisors, LLC
201-207-7935
aschanfield@verizon.net

January 23, 2014

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

Dear Ms. Woods:

I am pleased to provide the Financial Reporting Council (FRC) a summary of my commentaries on the recent consultation document "Risk Management, Internal Control and the Going Concern Basis of Accounting." (document)

In my opinion, this document meets the "gold standard" test. It is rich in content and thought throughout. Council members and those supporting them should be quite proud of this. I wanted to communicate this at the outset lest you interpret my remarks as being inconsistent with this overall conclusion. We have in our midst a piece of gold which just needs some "further mining and refining." Part of this richness is the consequence of years of thought leadership in this domain on the various governance, internal control and risk management codes issued by the FRC. As such I will not focus on the excellent areas in this document of which there are many.

First- I would strongly urge the Council to obtain a copy of HB 436 just released by Australia/New Zealand on how to implement risk management effectively. It is also quite rich in content and includes some key things I will focus on here relevant to the Board. This is a product of a working group under the Standards Australia and Standards New Zealand Joint Risk Management Committee. This is referenced at:

http://shop.standards.co.nz/catalog/436%3A2013%28SA%7CSNZ+HB%29/view or

http://infostore.saiglobal.com/store/Details.aspx?productID=1694350

The United Kingdom, Australia/New Zealand and Canada have a distinguished track record of providing leading edge thinking in risk management, internal control and governance. It is apparent that there is integrated thinking at the core of your consultation document which is

needed to deal with the complexities of this subject matter. These countries stand out unlike the United States which unfortunately made the strategic blunder of outsourcing its research in risk management to be outsourced to the large accounting firms and their proxies. At the core of my remarks, we need to recognize that there is a need to provide assurance to a wide variety of stakeholders as opposed to the very narrow focus we take here in the United States, which is opining on the financial statements.

Second- Nowhere in your document, do you provide a glossary of terminology which I think is critical to do. You use terms throughout such as identify, evaluate, manage, monitor, assess. Sometimes such terms are correctly used and sometimes not. I also see overlap and inconsistent usage. If you require specific examples, kindly let me know further. I suggest that you use the terminology from ISO 31000 (but ignore the ISO 31004 implementation guide) which you will find embedded in the HB 436 document. They use specific terms of identify, analyze and evaluate to describe the entire risk assessment process. They use treatment to describe how management responds to risk and they lay out specific terminology used in risk treatment. They use monitor and review to articulate management oversight and the independent assurance process.

The advantage in your using ISO terms is that it is rapidly becoming the world risk management standard and so your thinking will be in line with this standard and thus so helpful to many practitioners and companies that are just getting their hands around this subject matter. Most importantly, it is critical for Boards of Directors to be clear in their thinking. If for some reason, you are comfortable in using the terms you have used, then it would be most beneficial to include a glossary of terminology in the actual document.

Third- you state in Section 1- Introduction –under number 10 that "the guidance does not set out in detail the framework by which the company's principal risks are managed or mitigated or through which the board receives assurance." With all due respect to the FRC, this is one of the worst things you could possibly do as there currently exists guidance as specified in HB 436 on what "effective risk management means" and it would behoove you to use such guidance. Although companies will differ in terms of the type of risk management framework they implement, there will be commonalities such as the necessity of creating a comprehensive communication process with your key stakeholders and as well creating a risk management policy. These are just two examples but important ones. What will never change will be the risk management process and adherence to the key principles for effective risk management implementation. Specifically, effective risk management exists when the following two conditions are met:

- The Board, key management and other select stakeholders have a comprehensive, current and timely understanding of the risk portfolio
- The company is acting within the risk appetite/risk criteria set by the company

This should be a consistent standard that you establish- a bar so to speak. If you do not use such terminology, then what you will end up with at the Board level is a lot of bickering, inconsistent thinking and most importantly, an inability to compare one company to the next because of differing standards.

Fourth- I also reference you to a case study just prepared with two other colleagues that is being published shortly by John Wiley & Sons, and this will provide useful information for you. This book will be part of a best in class book of case studies on enterprise risk management as a companion to the highly successful *Enterprise Risk Management: Today's Leading Research and Practices for Tomorrow's Executives* (Wiley: 2010).

Fifth- You use the term principal risks but nowhere do you define it. For example, does it include a monumental risk which appears to be well mitigated thereby reducing the overall risk level to the company's risk appetite/criteria (i.e. residual risk) or does it only include monumental risks which exceed the authorized risk appetite/criteria of the company? Let us try to define what it is.

Other specific remarks which I have are as follows:

Appendix

Section 1 Introduction- 2- should say "good stewardship by the board must include sensible risk taking" instead of "should not inhibit." In the same paragraph where you say that the board and management should respond promptly to risks, I would say that it may not be necessary to immediately respond to a risk but it is necessary to promptly understand what the risk is and develop an appropriate risk treatment plan for it. Such plan could have executable steps which are immediate or not depending on the particular circumstances.

Section 1- Introduction- 11- you are not trying to achieve best practice but are trying to establish whether risk management is effective or ineffective. If a particular company is on target to have effective risk management, then this means that the company is following the risk management process, a well designed risk management framework, and is guided by specific principles. One such principle is culture and behavior and this should be auditable. But there are as well other key principles that are tied in with culture and behavior and thus need to be audited. For example, the principal of transparency and inclusiveness. I refer you to HB 436 for a list of the principles. Successful audit of the principles will lead one to conclude that a company either has effective or ineffective risk management.

Section 1- Introduction- 18- Where you state all reporting to the shareholders, do you mean to include reporting to other key stakeholders as well? There are certain stakeholders in companies that need to be kept apprised of events and risks within a company such as union officials,

environmental regulatory groups, etc. and as such limiting the reporting to only the shareholders will be insufficient to satisfy needs of the other stakeholders.

Section 2- Responsibilities- where you state that the board's specific responsibilities in relation to risk include determining the extent to which the company is willing to take on risk, it would make sense to indicate how you expect this to be expressed for each of the strategic objectives of the company. This then gets into the subject of risk appetite. Even though the regulators have been clamoring for use of this term, the term meaning how much risk we desire to take, is impossible to robustly put into practice other than for some of the key financial areas in a company. There are three key areas of problems in using risk appetite. These are conceptual, measurement and perceptual. Rather than get into extensive detail here on these three, I will refer you back to HB 436 which explains quite clearly how to implement risk criteria and why this is needed.

If you instead use the concepts and methodology of "risk criteria" this will allow you to define how much risk a company is willing to take in the pursuit of its objectives. Again I am willing to provide further examples to support my commentaries unlike many individuals in the marketplace that continually discuss risk appetite but are unable to provide a concise example of it throughout a business.

In the last bullet under number 19 under section 2 – should also take responsibility for internal communications on an as needed basis- somebody needs to make sure that there is a robust two way communications process with the internal stakeholders. Are you suggesting or inferring by absence of remarks that the Board does not have responsibility for this? What about for example, roll out of the entire risk management program? Or what about communications with the CEO from the top down or announcements of major acquisitions just as some examples?

An external party reviewing the risk management system should as well report on performance of the Board and some guidance should be provided on parties qualified to perform such reviews. I did not see either of these areas discussed in your document. Some suggest that such parties be the internal auditors and whereas conceptually this makes sense, to date generally speaking, they have not demonstrated the skill sets to do so. Not that many other parties have either done so. The point is that the Board should determine what level of review must be performed and have identified qualified independent parties to do so.

Section 4- number 25 – It should not be the Board that identifies the principal risks. The Board should ensure that all of the principal risks have been identified accurately and timely, one of the two criteria for effective risk management as noted above.

Section 6- Number 36- Where you state "that the Board should form its own view on effectiveness based on the evidence it obtains, exercising the standard of care generally applicable to directors in the exercise of their duties", this will be impossible to do well without

implementation of my recommendation of above on establishing criteria for what effectiveness means.

In the section for Questions for the Board to Consider

Risk Appetite

1st bullet under risk appetite and culture- "what risks is the board willing to take and what risks will it not take." This sounds great in theory but you will be unable to execute this without deploying use of term "risk criteria" as noted above.

3rd bullet under risk appetite and culture- on whether the Board has the requisite skills, etc. You should also add the question requiring elaboration as to basis for this conclusion.

The Risk Management and Internal Control System

1st bullet –should add at end after coordinated "and documented in the company's risk management policy"

I hope that my commentary has been helpful to you. I look forward to seeing your final document and of course reading the commentaries by other risk management practitioners. As stated above, feel free to reach out to me should you require further clarification on any of my points.

Sincerely yours,

Arnold H Schanfield, CIA, CPA

Principal of Schanfield Risk Management Advisors, LLC