Hong Kong Institute of
Certified Public Accountants
香港會計師公會

30 September 2016

Our Ref.: C/TXG, M107889

COSO Board and Principal Contributors

Dear Sirs,

COMMENTS ON THE EXPOSURE DRAFT ON THE ENTERPRISE RISK MANAGEMENT – ALIGNING RISK WITH STRATEGY AND PERFORMANCE (JUNE 2016 EDITION)

The Hong Kong Institute of CPAs ("Institute") appreciates the Committee of Sponsoring Organisations of the Treadway Commission ("COSO")'s long-standing work in the important area of organisational risk management and internal control. We also welcome the opportunity to comment on the Exposure Draft ("ED") of the updated enterprise risk management ("ERM") framework, from the perspective of a professional body whose members may be responsible for different aspects of the development and operation of an ERM system in their own organisations, and who would welcome additional guidance in this area.

We support the aim of the current work of COSO to build on and further develop the existing COSO ERM framework. In our view, there are certain further enhancements that could be made to the proposed framework in the ED that would help to make it a more effective and usable model. Our comments on the ED have been set out below for your easy reference.

A. High-level comments

i. Whilst is stated in the ED that the framework is applicable to organisations of all sizes, it would be helpful to indicate through examples how it can be scaled to different sizes/ types of organisations. In places, the model may be perceived as being "over-engineered", particularly for small and medium enterprises, given the extensive explanation of 23 principles. We would suggest that COSO consider producing application guidance on ERM for smaller businesses, as has been done with the internal control framework.

ii. The ED contains useful concepts that will help stimulate organisations to think about the key issues in relation to their own ERM. Many of the ideas and themes in the ED merit further elaboration and exploration, but more may need to be done to crystallise the various strands of thought into a clear and systematic whole.

iii. Given the apparent objective to provide a framework for all types of organisations, it is understood that a balance must be struck between outlining general concepts and principles and delving into more specific areas. As the ED favours a more conceptual approach, this tends to leave gaps, where more practical advice and guidance would be welcome. These include:

- Governance structure and board responsibilities, and what boards need to know to fully discharge their duty. This could, for example, try to draw lessons from the global financial crisis and to ask, what could have been

37th Floor, Wu Chung House,
213 Queen's Road East, Wanchai, Hong Kong
香港灣仔皇后大道東213號胡忠大廈37樓
Tel電話: (852) 2287 7228
Fax傳真: (852) 2865 6776
(852) 2865 6603
Website網址: www.hkicpa.org.hk
Email電郵: hkicpa@hkicpa.org.hk

done better, in terms of risk identification, assessment and management, and how adopting effective ERM could help to address those issues.
- Ensuring procedures, processes and accountabilities, etc. cascade down from the board, through the management to divisions and units, and individual roles, etc.
- The important issue of what should be reported internally and externally is worthy of more detailed and specific coverage.

iv. Following on from the above, it would be helpful if the ED were to make it clearer what subsequent steps organisations may need to take: E.g., does the framework seek to be sufficient for organisations to directly implement an ERM system, or it is envisaged that organisations will still need to develop additional implementation procedures and processes for their own environment, by drawing on or adapting the framework?

v. While boards, chief executives and senior management should find the Executive Summary a valuable general overview of the framework, it would be questionable to suggest, or give the impression, that reading the Executive Summary alone is sufficient for their purposes. Directors and senior management should invest the time to understand the proposed ERM model in more detail, otherwise the goal of integrating ERM into strategy setting and even, as some others have suggested[1], into the development of an organisation's mission and vision, and making clear where ultimate responsibility and accountability lie, may not be achieved. This should be one of the lessons learned from the global financial crisis.

vi. We would suggest that the aim should be, at some later date, to integrate the COSO ERM and internal control frameworks, because, increasingly, risk management internal control are seen as facets of a single integrated activity rather than as discrete functions.

B. More detailed observations

1. Overall aim of the ED: The concepts and principles of enterprise risk management set out in ED are intended to apply to all entities regardless of legal structure, size, industry, or geography. Undoubtedly, all enterprises need to take risk into account in formulating their business strategies, but smaller enterprises may adopt simpler approaches in their formulation of business strategy and, in implementing an ERM system. They may not be able to follow the model in its entirety.

2. The existing COSO 2004 ERM model places greater emphasis on the involvement of different parties in the ERM process. ERM is defined in the 2004 framework as follows:

"Enterprise risk management is a process, effected by the entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of objectives."

[1] We note the comments on the ED from internal auditor, author and blogger, Norman Marks, and would agree with a number of them

The ED now proposes to include risk culture and capability within the definition of ERM, which is defined as:

"The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organisations rely on to manage risk in creating, preserving and realising value."

It is a welcome development that the new definition in the ED highlights the importance of organisational risk culture and capability, and the integration of risk awareness into strategic decision making. Corporate culture is certainly important in implementing ERM. If there is strong resistance to change, inefficient communications and a poor reporting culture in an enterprise, it would be difficult for that enterprise to implement an effective ERM system.

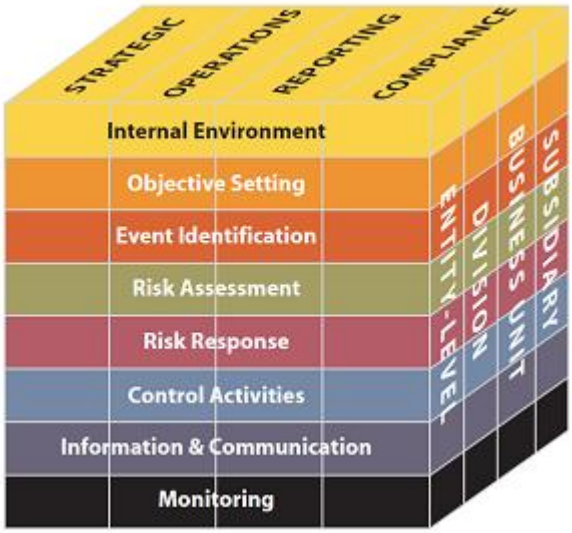
On the other hand, while the reference to the roles of various parties in the 2004 definition is ultimately very broad, covering as it does, the board, the management, and other personnel, arguably one of the weaker areas of the ED is the apparent downgrading of the explanations of roles and responsibilities, which are relegated mainly to an appendix.

3. The key part of title of the ED, *Aligning Risk with Strategy and Performance*, in our view, could have provided a clearer reflection of the objective of the ERM framework: E.g., integrating risk and opportunity into decision making - to improve strategy development and performance. This may be indicative of the need to give the framework a sharper focus.

4. The figure below and modified versions of it appear at different places in the ED, as replacement for the cube representation used in the 2004 framework.

Figure 3.1: Strategy in Context

Below is the cube diagram used in the COSO 2004 framework to summarise the ERM model.



While the ERM graphic in Figure 3.1 may have undergone a more contemporary "makeover", and seek to convey a more dynamic process than is suggested by the static-looking cube, it is debatable whether the 2004 cube should be dispensed with altogether. The latter offers a fairly effective illustration of the interrelations between various elements in the ERM environment.

We would suggest that one option may be to retain a modified version of the cube alongside a version of the latest graphic.

5. The framework would be enhanced by the addition of further practical guidance. In the introduction (chapter 1), paragraph 3 states: "Management has many choices in how it will apply enterprise risk management practices, and no one approach is better than another. However, readers who may be looking for information beyond a framework, or different practices that can be applied to integrate the concepts and principles into the entity, will find the appendices to this publication helpful."

   Organisations may find the general statement above to be too open ended as guidance, because it would suggest, in effect, that ERM can be applied as organisations see fit and that there is no right approach. Furthermore, the information referred to in the appendices may not be sufficiently extensive to serve as implementation guidance.

   One of the two main appendices, Appendix B, looks at roles and responsibilities (the other, Appendix C, provides illustrations of risk profiles). There is relevant information on possible structures for oversight and accountability for ERM in Appendix B, and probably some of this should be included in the main body of the framework, but the proposals avoid taking any position or advising on the appropriate oversight/ governance set up, as illustrated by the following statement, among others:

"Some industries offer specific guidance for implementing an accountability model, but organisations must consider factors such as their size, strategy and business objectives, organisational culture, and external stakeholders."

This tends to dilute the effect and, prima facie, would allow boards to opt to distance themselves from the process. Additional practical advice on actions that organisations can take to ensure that ERM awareness and understanding permeates throughout the organisation, and that the risk identification, assessment and management processes cascade down from entity to unit level, etc., would be highly beneficial.

6. In chapter 3 on ERM and strategy, at paragraph 46, passing reference is made to risk associated with an organisation's mission and vision, but this is not further explored. The focus of the ED is on risk associated with strategies and achieving objectives. This is a potential gap (identified also by others. See the footnote on page 2).

7. Figure 5.2 in chapter 5, on components and principles of ERM, provides a good summary of the proposed model.

8. The emphasis on risk culture, which is new (chapter 5 is on risk governance culture), is important, in the same way that establishing a sound corporate governance culture is a prerequisite for embedding good corporate governance within an organisation. Para. 94 is evidence that the proposed ERM model is considered to be appropriate for all types of entity: small family-owned private companies, large, complex multinationals, government agencies and not-for-profit organisations; hence, perhaps, the reluctance to step beyond the provision of high level concepts and principles.

9. Principle 1, on board risk oversight (paras. 95-103): This would be an opportunity to say more about the importance of board members having the capacity, time and sufficient information to understand the nature and extent of risks assumed by the organisation. "Organisational bias" is referred to in para. 103. Possible bias is also referred to in various places in the ED (e.g., para. 278, under principle 13 on assessing the severity of risk, and para. 291 in relation to prioritising risks). It would be worthwhile to elaborate on the nature of possible bias, the impact that this may have on ERM and how this can be addressed.

10. Principle 2, on establishing the governance and operating model (paras. 116-117) refers to the fact that ERM considerations may evolve with technology. Further elaboration or guidance on this potentially important area would be welcome.

11. In principle 3, on defining desired organisational behaviours (paras. 121-122), the ED indicates various factors that shape entity culture. It goes on to say that “these factors influence where the entity falls on the culture spectrum, which ranges from averse to risk aggressive. The closer that an entity is to the risk aggressive end of the spectrum, the greater is its propensity for and acceptance of the types and amount of risk necessary to achieve strategy and business objectives.” Without further explanation, this appears to be a relevant but questionable assumption, i.e., that entities need to be more risk aggressive to achieve their strategy and business objectives. It also does not seem to be borne out by the first part of the example (Example 6.2) to which it refers, which quotes the case of a nuclear power station.

12. Under principle 12, on identifying risk in execution (para. 245), advice is offered on descriptions of risk. This is an example of how the framework can be quite practical and additional advice of this nature would certainly be valuable. Paras. 247-249, under the subheading of *the scope of identification* relates to the need to implement ERM processes at all levels of an entity. There are a number of other such references in the ED (e.g., paras. 258, under assessing the severity of risk, and 306 on developing a portfolio view) and, therefore, more detailed explanations of how to link up and integrate ERM throughout an organisation, etc. would help readers.

13. Identifying potential opportunities is also touched on (para. 253) and there are other passing references (e.g., para. 303, under identifying and selecting risk responses) but, generally, the more positive aspects of effective ERM in terms of opening up opportunities is not explored very much, as others have noted.

14. Under principle 19, on leveraging information systems (paras. 345-346), it would be useful if the ED were to provide examples of risk management taxonomies.

15. Under principle 20, on communicating risk information, again, more detail and guidance could usefully be provided on this very important area of ERM. In relation to the board, para. 361, for example, simply states:

    "Management provides any information that helps the board fulfil its oversight responsibilities concerning risk. There is no single correct method for communicating with the board but the following are some common approaches..."

    While some useful examples are then provided, it would seem appropriate here to emphasise the importance of the management providing sufficient, timely information, clear and relevant information to the board. In para. 366, the fact that many organisations have whistle-blowing policies and protocols for raising concerns about irregularities is noted without comment. However, on the face of it, these are potentially valuable tools in an ERM framework.

16. Appendix B, on roles and responsibilities, contains some useful information, some of which could be relocated to the main body of the ED. However, there is a sense that the emphasis is on the responsibility of the management rather than on the board although, in many jurisdictions, legal responsibility rests with the board. Para. 405, for example, states:

    "Management is responsible for all aspects of an entity, including enterprise risk management."

17. More generally, the ED uses simple examples rather than more concrete business cases to illustrate key concepts. Experienced risk managers would be able to associate the key concepts mentioned in the ED with real life situations. However, some readers may find it difficult to appreciate why some of the elements mentioned in the ED are important in the ERM context. Further elaboration of certain topics may be required to help bring the concepts alive for readers with less working experience.

18. Coverage of certain increasingly important risk-related topics in the ED may merit some further discussion. As regards information technology, for example, data management is discussed briefly under principle 19 in the ED. Data architecture and management are very important to entities and data is a valuable asset for many enterprises. It is essential to ensure that data is safe and robust. System security (hardware, software, firewalls, user access right, user authentication issues, etc.) is an area that should perhaps be covered to some extent in the ED. Big data and business analytics are also common information technology priorities in corporate environment these days. Many enterprises include these in their strategy formulation and risks are associated with deployment of these tools.

19. As indicated above, we would go along with a number of the issues by others on the ED; for example, regarding whether the ED should devote more time to exploring the opportunities arising from uncertainty as well as the potentially negative side of risk; whether the update will provide the structure and guidance decision makers need to determine the right balance between risk and reward, and make effective decisions in real-life situations; and whether the guidance will be sufficient to enable board or relevant board committees to provide effective oversight.

The comments above are intended to be constructive and to make suggestions on where further information, explanations or examples would, in our view, add to the effectiveness of the COSO framework. We are supportive of the objectives of COSO in helping organisations to increase their risk awareness and understanding of how effective risk management can improve the processes and quality of decision making and strategy development, and benefit organisational performance.

The provision of additional implementation guidance, including guidance for smaller businesses, would be consistent with the above objective and would no doubt help facilitate the adoption of the COSO model.

Should you have any questions on this submission, please feel free to contact Peter Tisman, director advocacy and practice development, at the Institute on (852) 2287 7084 or by email at: peter@hkicpa.org.hk.

Yours faithfully,

Peter Tisman
Director, Advocacy and Practice Development

PMT/EKC/ay