International Federation of Accountants®

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.ifac.org

September 30, 2016

Robert Hirth
Chairman
Committee of Sponsoring Organizations of the Treadway Commission
Via upload link

Re: Comments on *Enterprise Risk Management—Aligning Risk with Strategy and Performance*

Dear Mr. Hirth,

Within organizations across the globe, many professional accountants in business are in a position of strategic or functional leadership, or are otherwise well placed to partner with other disciplines in the implementation, execution, evaluation, and improvement of organizational risk management arrangements. In addition, many professional accountants in business have the responsibility to provide objective, accurate, and timely information and analyses to support good (risk) management. Therefore, the Professional Accountants in Business (PAIB) Committee of the International Federation of Accountants (IFAC) values the opportunity to comment on the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s Exposure Draft of the update to its *Enterprise Risk Management–Integrated Framework* ("ERM Framework").

With the increased volatility in the modern business environment and the recent financial and economic crises around the world, the effective management of risk in organizations—including good internal control—has taken on even greater importance. Effective risk management facilitates the achievement of an organization's objectives, while complying with legal, regulatory, and societal expectations, and enables the organization to better respond and adapt to surprises and disruptions. IFAC, therefore, commends COSO on taking up the challenge to update its ERM Framework.

IFAC also greatly values COSO's invitation to participate in the Advisory Council to this project, which has allowed us to actively contribute to all stages of the update process. IFAC is happy to see that many of its views on the effective management of risk are reflected in the current draft, especially with the *Executive Summary* stating that "integrating enterprise risk management into an organization helps to accelerate growth and enhance performance by more closely linking strategy and objectives to both risk and opportunity." This is closely aligned with IFAC's recent thought paper, *From Bolt-on to Built-in*, which argues that organizations should primarily focus on setting and achieving their objectives to create sustainable value and growth and that managing risk, both positive and negative, is a natural and integral part of that.

IFAC also supports many of the other intentions for the updated ERM Framework, as expressed in the *Executive Summary*. For example, it supports the ideas that:

- Organizations need to become more anticipatory and adaptive to change, which may create both opportunities and threats;

- ERM should take into account the expectations of a multitude of stakeholders;
- Integrating ERM throughout an entity provides a clear path to creating, preserving, and realizing value;
- Effective ERM supports all levels of entity decision making in the face of uncertainty in strategy and execution;
- Risk should not be viewed in isolation, but in the context of an organization's objectives; and
- Therefore, ERM should appeal to all Board members, managers, employees, and other stakeholders in entities—not just the chief risk officer.

We also like the new signature ERM graph (the replacement of the "cube"), as it nicely depicts how effective ERM interrelates with an entity's mission, vision, and core values, how it affects the entity's performance, and how it is integrated into strategy planning and day-to-day decision making. So, all in all, we support the *Executive Summary*.

Align ERM Framework with Intentions from Executive Summary

The biggest challenge that we encountered, however, is that the actual ERM Framework itself currently does not yet sufficiently live up to the intentions (or aspirations) as described in the *Executive Summary*. For example:

- The thrust of the draft is still about risk management as a separate activity, speaking predominantly in terms of identifying and managing individual risks, as opposed to an activity that's integrated within the decision-making process.
- The document is still overwhelmingly about mitigating threats and light on capturing opportunity. Often, risk is solely depicted as adverse, without including the opportunities to enhance and grow the business.
- Notwithstanding the new signature graph, the underlying components and principles are almost a duplicate of the internal control integrated framework model and, as such, not very new or inventive.
- The text of the ERM Framework is too long, contains relatively technical language and inconsistent (use of) terms, and is not particularly readable. This inhibits understandability and ease of use, not only for people working at the Board and management level, but also for those in a more operational role. This is important, as reading an executive summary could never be a substitute for reading a document in its entirety.

- The approach is quite inward-looking. The Board and management set risk appetite, tolerance, etc., but surely this has to be communicated to, and indeed discussed with, owners, funders, and other stakeholders.

- Various parts of the guidance seem very theoretical and over-engineered and, for that reason, difficult to relate to how Boards, managers, employees, and other stakeholders go about meeting their responsibilities in the real world.
  - A topic that comes to mind is the division of strategic risk in "The possibility of strategy not aligning," "Implications of the strategy chosen," and "Risk to executing the strategy" (see Chapter 3), which is difficult to understand.
  - Another example is the discussion on risk profiles in Chapter 4. We are really not convinced about the usefulness of the heavy emphasis on plotting a point on a graph, which comes across as a bit of pseudo-science and is the sort of thing that gives ERM a bad name.

  While the former could probably benefit from a thorough rewrite, the latter seems more conceptually flawed[1] and is also unnecessary for instilling a good understanding of how risk affects objectives (performance) and how it can be effectively managed.

- At the moment, the ERM Framework comes across as somewhat formulaic and linear, rather than a more "messy" iterative process where continuous learning is key. The final Framework needs more emphasis on culture, capabilities, and behaviors. It would also be useful to link the Framework to a broader range of tools and practices, e.g., "where to find out more on xx." This helps to emphasize the point that the framework is not "one size fits all."

- The components of the ERM Framework are inconsistent with the correct assertion in the *Executive Summary* that organizations should integrate ERM to obtain the full range of benefits/to be effective. Instead, the components in the ERM Framework deal with:

  - "***Risk*** Governance" as a separate activity, rather than how ERM should be organically integrated into the (overall) governance and business model of an organization.

  - "***Risk*** in Execution," encouraging risk listing and developing risk registers, rather than keeping the organization focused on the objectives to be achieved while managing the related risk (or uncertainties).

  - "***Risk*** Information, Communication, and Reporting," creating a whole new and separate information stream, rather than integrating risk into the already existing managerial information, communication, and reporting processes.

[1] The diagrams in Section 4 seem to depict a correlation between risk and performance (when organizations increase risk, they crank up performance), whereas there is more likely a relation between expected benefits and the amount of risk that organizations want to assume to receive them.

- "Monitoring *Risk Management* Performance,"[2] as opposed to managing overall organizational performance to assess how risk affects an organization's efforts of creating, preserving, and realizing value.

We are concerned that the current Exposure Draft of the ERM Framework is not yet sufficiently thought through to really shape "the culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value."[3]

Arguably, the most pivotal change to be made to align the ERM Framework with the intentions as voiced in the* Executive Summary *would be to reverse the perspective from risk based to (strategic) objective based: placing organizational strategy and execution at the forefront and then showing how organizations could actually integrate the management of risk into their (already existing) "culture, capabilities, and practices."

Once this reversion has taken place, the various elements of the ERM Framework, such as the components and principles, will almost automatically fall into their new place: not as separate, add-on activities but as important pointers to influence the managerial processes that already exist—to enhance and improve them but not necessarily replace or increase them.

Such an approach would also correspond with the main objective of an organization, which is *not* to effectively manage risk, *nor* to have effective controls, but to ensure that it makes the best decisions and achieves its (strategic) objectives.

Align ERM Framework with other risk management standards

Various other standards, frameworks, and guidelines are available to assist organizations in evaluating and improving their risk management arrangements, on a global level most notably the standard *ISO 31000:2009, Risk management – Principles and guidelines*.

Many organizations, not only multinationals, use various sources for developing their risk management arrangements. Further international alignment of the underlying terms and concepts—as a minimum reconciling contradictory or conflicting recommendations[4]—would facilitate their continuous improvement efforts, reduce costs, and allow for the comparison of these arrangements across borders and, thus, increase stakeholder confidence.

In many other areas, such as financial reporting or auditing, global convergence has been underway for years. For governance, risk management, and internal control, however, is it still in its infancy. As the ISO

---

[2] Of course, an organization should also monitor the effectiveness of its risk management arrangements itself, but this is of a different order than managing risk in the primary process of setting and achieving an organization's objectives.

[3] = COSO's new definition of ERM.

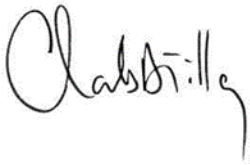
[4] For example, the key terms "risk," "inherent risk," "risk appetite," and "uncertainty."

31000 standard is currently also under revision, we urge both COSO and ISO to actively engage with each other to identify and resolve all significant issues that might rise.

Detailed Comments

For the convenience of the development team, we have included our comments on the specific questions outlined in the COSO Feedback Document in Appendix A. In addition, we will send you a few editorial suggestions under separate cover. We hope you find them useful while finalizing the ERM Framework. Please do not hesitate to contact me should you wish to discuss any of the matters raised in this submission. We also welcome further discussions on how IFAC can continue supporting the important work of COSO.

Yours sincerely,



Charles Tilley
Chairman, IFAC Professional Accountants in Business Committee

About IFAC and the PAIB Committee

The International Federation of Accountants® (IFAC®) is the global organization for the accountancy profession dedicated to serving the public interest by strengthening the profession and contributing to the development of strong international economies. It works with its member organizations around the globe to achieve this goal. Through its current membership of more than 175 professional accountancy organizations in more than 130 countries and jurisdictions, IFAC represents nearly 3 million accountants in public practice, industry and commerce, government, and education.

The IFAC PAIB Committee provides leadership and guidance on relevant issues pertaining to professional accountants in business and the business environments in which they work. Within organizations across the globe, many professional accountants in business are in a position of strategic or functional leadership, or are otherwise well placed to partner with other disciplines in the planning, implementation, execution, evaluation, or improvement of internal control. In addition, many professional accountants in business have a responsibility to provide objective, accurate, and timely information and analyses to support all of these activities.

International Federation of Accountants®

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.ifac.org

Appendix A: Comments on the specific questions outlined in the COSO Feedback Document

Name: Charles Tilley
Email:VincentTophoff@IFAC.org
Stakeholder group: Accountancy profession
Organization name: International Federation of Accountants (IFAC)
Industry sector: Not-for-profit
Geographical region: Global

Question 2. Are you a member of one or more of the following organizations?
Other relevant organization. IFAC is the global organization for the accountancy profession dedicated to serving the public interest by strengthening the profession and contributing to the development of strong international economies.

Question 16. Regarding the Executive Summary:

- The Executive Summary is appropriately written for an audience of boards and senior management: (strongly) agree
- The Executive Summary is a suitable length: (strongly) agree
- The Executive Summary provides a sufficient overview of the Framework: disagree
- The Executive Summary clearly describes the strategic value of enterprise risk management: (strongly) agree

Comments: The ERM Framework is not aligned with the (intentions as described in the) *Executive Summary* (see our main comments). As such, the *Executive Summary* is not a summary.

Question 17. The Framework is appropriately detailed for risk practitioners and those applying enterprise risk management practices: disagree

Comments: *Everyone* in an organization should apply risk management practices, as per the assertions in the *Executive Summary*. The ERM Framework is not only too detailed, too long, and too theoretical, the main issue is that it describes a separate risk management process ("add-on"), rather than explaining how the management of risk should be integrated into the already existing overall system of management ("built-in").

Question 18. The Framework is scaleable and applicable for the following entities:
Small: disagree
Large: disagree
Not-for-profit: disagree
Government: disagree

Comments: All organizations, regardless their type, form, or size, need all elements of good risk management to be properly integrated into their system of management. The current *Executive Summary* is pointing in the right direction. The current ERM Framework is, however, written from a large organization perspective, which is likely to make it hard for smaller enterprises to engage with it.

Question 19. The definition of enterprise risk management:
[The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value]:

Comments: Please engage with ISO 31000 and other issuers of ERM guidelines to ensure international alignment of the underlying terms and concepts—as a minimum, reconciling contradictory or conflicting recommendations.

Question 20. The Framework will be relevant for the next 10 years: disagree

Comments: Risk management arrangements, as asserted in the *Executive Summary*, will be relevant for the next 10 years and beyond. As explained above, however, the current ERM Framework does not yet live up to that.

Question 21. The Framework provides an appropriate balance of international perspectives: disagree

Comment: Although IFAC greatly values COSO's invitation to participate in the Advisory Council to this project, we also note that the full COSO Board, as well as most people from the PwC Development Team and the Advisory Council, have a US background. In addition, we know and appreciate that COSO has reached out internationally to receive stakeholder input at the start of the update project and now also has issued this Exposure Draft for international stakeholder feedback. But, to our knowledge, no substantial dialogue has taken place with other international issuers of standards, frameworks, and guidance in the risk management area. As mentioned above, we would strongly advise you to engage in such dialogue.

Question 22. The Framework's 23 principles provide a comprehensive depiction of enterprise risk management: disagree

Comment: As noted in our overall response, the current 23 principles still provide more of a siloed, rather than an integrated, depiction of enterprise risk management.

Question 23. The following components enhance the reader's understanding of enterprise risk management:

Comment: All of the components, as formulated, are still too much skewed toward a siloed, rather than an integrated, understanding of enterprise risk management. See also our general comments above.

Question 24. Internal control is an integral part of enterprise risk management: fully agree

Comment: Effective enterprise risk management, in turn, is an integral part of an organization's overall system of management, and the updated ERM Framework should reflect that more than it currently does.