The Institute of Internal Auditors Global

September 26, 2016

Response submitted online via the upload link

Re: Enterprise Risk Management — Aligning Risk with Strategy and Performance

On behalf of more than 185,000 global members of The Institute of Internal Auditors (IIA), I am pleased to provide our response to The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Exposure Draft, *Enterprise Risk Management — Aligning Risk with Strategy and Performance.* As a founding sponsor of COSO, we appreciate the opportunity to participate in this comprehensive revision. We greatly value the involvement and contributions of two IIA representatives appointed to the Advisory Council for this project. As well, The IIA's president and CEO serves an important role as one of the COSO board members.

Our comments were guided by a team of leaders in the internal audit profession representing The IIA's global reach. We were pleased to observe many notable improvements proposed for the *Enterprise Risk Management—Integrated Framework* with this update project (Updated Framework). At the same time, we believe there are opportunities for further refinements that deserve consideration. Our key observations follow.

## Improvements in the Updated Framework

### 1. Aligning risk with strategy and performance.

The new title for the Updated Framework, *Enterprise Risk Management—Aligning Risk with Strategy and Performance* is illustrative of a major step forward with this update. For enterprise risk management (ERM) to be truly effective within an organization, it must be an integral part of how business is done and have a strong relationship with value creation and value preservation. This critical underpinning is supported by a number of concepts brought out in the Updated Framework, to include a focus on "improved decision making," "enhanced performance," and linking "strategy and business objectives to both risk and opportunity." For example, paragraph 376

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.globaliia.org

states that, for risk reporting to the board, "it is critical that the focus of reporting be the link between strategy, business objectives, risk, and performance."

**2. Improved clarity, structure, and relevancy.**

The Updated Framework is much clearer and better structured with the use of principles organized into five interrelated components. As well, the definition of ERM as being "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" is both comprehensive and precise. The diagram depicting the relationships from an organization's mission, vision, and values through to enhanced performance (Figure 3.1) is a strong representation of the context within which ERM can support the achievement of an organization's strategic and business objectives.

**3. Recognition of the importance of culture.**

In recent times, recognition of the important and pervasive role organizational culture plays in everything the organization values, prioritizes, and does has come to the forefront. A strong, positive improvement was made by highlighting the critical role culture plays in establishing an organization's tone and orientation to ERM as a prominent element of the Updated Framework's first component.

**4. Enhanced terminology.**

ERM terminology, such as risk appetite, risk capacity, and risk tolerance, can be confusing. The Updated Framework makes good progress clarifying and explaining ERM terms. For example, we noted introduction of the concept of "acceptable variation in performance" over the use of the much misunderstood and confusing term "risk tolerance." Making risk tolerance more about the range of acceptable performance and not just about a maximum value an organization is willing to "tolerate" is a notable clarification and a valuable improvement.

**5. Use of examples and illustrations.**

In many cases throughout the update, the clarification of critical concepts with tangible examples and narrative illustrations helps to avoid mere articulation of technical jargon and will aid the reader to better comprehend the content.

**<u>Areas for Further Consideration with the Updated Framework</u>**

**1. Risk is more than a negative to minimize or avoid.**

The text supporting the Updated Framework is clearly more balanced when it comes to recognizing the upside of taking well-informed risk, and that risk is not a bad thing that should be minimized or avoided at all cost. However, there are sections in the document where this balanced view is not sufficiently recognized, with language conveying risk as predominately something to minimize or avoid. When making decisions to achieve its objectives, an organization makes choices from a range of options (including not doing anything at all). Each choice involves risk and each choice can have a beneficial or detrimental effect, or both. For example, Principle 12: Identifies Risk in Execution, exclusively uses negative terms (see paragraph 242), and Example 7.9: Making Changes to Strategy, at paragraph 205, uses the phrase "mitigates the risk" to describe an

outcome of the strategy, without articulating that the change in strategy also was made in "pursuit of an opportunity." We suggest that more examples of the upside of smart risk-taking as part of effective risk management would better emphasize the point that risk is also something to be wisely exploited to an organization's benefit.

**2. Give more consideration to the complexity of assessing risk.**

In its most rudimentary sense, risk is generally viewed as the intersection of likelihood and impact. This is how many organizations historically think about assessing risk, and how much of the Updated Framework is oriented. However, the concept of assessing risk could be better developed to enable the Updated Framework to advance ERM and not simply codify current practice. Concepts such as quantifying risk, scenario analysis, distribution of variation in performance (instead of only a point estimate of risk), residual risk, and distinction between risk severity and risk prioritization factors are difficult to comprehensively incorporate into an organization's ERM activities. Given the complexity of assessing risk in actual practice, we would like to see these advanced considerations explored more thoroughly. If not addressed in the Updated Framework, then a separate and more detailed document addressing these complexities should be considered.

**3. Better explain what is meant by taking a "portfolio view."**

The development of an organizational risk profile is a solid and foundational theory, but it is extremely complex to implement in actual practice. The understanding of risk in an organization is rarely as simple as the Updated Framework implies (Figure 8.4). Organizations have multiple risks, usually involving multiple interdependencies. The Updated Framework introduces the concept of taking a portfolio view of risk, which is appropriate. The application of risk appetite, risk severity, interdependencies, and other aspects of ERM need to be addressed at the portfolio view. However, for most organizations, a portfolio view of risk can be much more complex. We believe the conceptual and theoretical coverage of the portfolio view of risk in the Updated Framework (both in Principle 16: Develops Portfolio View and in the corresponding appendix) is not sufficiently detailed to be implemented effectively. If not addressed in the Updated Framework, then a separate and more detailed document that comprehensively addresses this complex topic should be considered.

**4. Acknowledge the role of internal audit in risk management.**

Principle 23: Monitors Enterprise Risk Management appropriately emphasizes the need to monitor ERM activities. However, the discussion addresses only the types of improvements that could be identified and made to ERM, not the process for the monitoring itself. There are different levels, types, and characteristics of monitoring. Further discussion of the objectives and attributes of different types of monitoring, including the role of internal audit in monitoring and assessing the performance of ERM, should be added. Internal audit should, and in an increasing number of organizations does, play a crucial role in providing assurance over an organization's risk management practices and processes. In addition, in the section on types of reporting and risk reporting to the board (paragraphs 374 through 376), examples of supplemental risk reporting by subject matter experts is raised (most specifically in paragraph 374). Examples listed are compliance, legal, and technology. The role of internal audit in reporting on risk to management,

the audit committee, and the board, leveraging its independence and objectivity, as well as its broad organizational purview, should be brought out in this section.

**5. Add comprehensive examples.**

The Updated Framework provides many examples that are extremely helpful in understanding the stated concepts. However, implementing and improving upon ERM is an extremely complex topic, especially in how it is integrated into all aspects of decision making and includes a multitude of interdependent risks. Consideration should be given to developing separate documentation that provides comprehensive examples, taking the reader through the entire ERM process in different types of example organizations.

**Other details and technical observations**

We noted a number of detailed technical observations in terms of word choice, unnecessary language, and lack of clarity and specificity that we will provide to the drafting team under separate cover.

Thank you for the opportunity to provide comments on *Enterprise Risk Management — Aligning Risk with Strategy and Performance.* Please do not hesitate to contact Francis Nicholson, The IIA's Managing Director of Global Advocacy, if you have any questions about this response or would like to schedule a time for discussion. Mr. Nicholson can be reached at francis.nicholson@theiia.org or +1-407-937-1236.

Best regards.

Angela Witzany, CIA, QIAL, CRMA
Chairman of the Board