risk oversight solutions
A better response to risk.

Comments on the June 2016 COSO draft "Enterprise Risk Management: Aligning Risk with Strategy and Performance"

Thank you for the invitation to provide comments on the June 2016 COSO exposure draft "Enterprise Risk Management: Aligning Risk with Strategy and Performance". ("ED") Based on my detailed review of the three COSO documents that comprise the ED I believe that this update represents a major improvement over COSO ERM 2004. The development and advisory teams have made significant improvements and positive direction changes. Having said that, I still believe major changes and clarifications are required if the rapidly escalating needs of key stakeholders, including boards, senior management, risk and internal audit specialists, regulators, shareholders, the general public, and others are to be better served.

My comments are drafted from the perspective of a consultant, ERM software designer, trainer, and author that has worked globally over the last 30 years with hundreds of public and private sector organizations interested in implementing ERM. I have expert level knowledge related to the 1992 and 2013 COSO integrated control frameworks, COSO ERM 2004, ISO 31000 2009 global risk management standard, the extensive work done by the Financial Stability Board and global senior supervisors to study root causes of the 2008 financial crisis and develop risk governance guidance for regulators globally, and governance and risk regulatory frameworks in Canada, the U.S., and the UK. My work in the space has been recognized with Outstanding Contributor awards from the Ontario CPA/CA institute in Canada, IIA Canada, IIA Global, and the ACFE. My articles on board oversight of risk and the need for radical changes in status quo ERM and internal audit methods have been published in The Handbook of Board Governance, Conference Board Director Notes, Ethical Boardroom, Harvard and Columbia Law Governance Blogs, Internal Auditor magazine, Governance Institute of Australia, the National Post, and many others.

My remarks have been drafted at a macro level with the sincere hope they will significantly influence the direction the COSO ERM development team takes in the final guidance. I would be happy to meet in person to provide more details and support for my observations and recommendations if there is interest.

Sincerely,

Tim Leech FCPA CIA CRMA CCSA CFE
Managing Director

216 CARLINI COURT, SUITE 201, OAKVILLE, ONTARIO, CANADA, L6K 3Y8 (T) 416.720.0392 (F) 905.337.3627
www.riskoversightsolutions.com

Concern #1 – LACK OF RESEARCH ON CAUSES OF ERM FAILURES – the FAQ release of the updated June 2016 COSO ERM documents indicates on page 4/10 that some effort has been made to analyze ERM implementation "challenges", "critical issues", and "concerns".

Assess and Envision – Through literature reviews, global surveys, and public roundtables and forums, this phase identified current challenges for organizations implementing enterprise risk management. During this phase, PwC analyzed information, reviewed various sources of input, and identified critical issues and concerns. COSO launched a global survey, available to the general public, for providing input on the original Framework, soliciting almost 900 responses.

A new guide, a very good one that could compete with the COSO ERM guidance if it had elevated authoritative stature, has been issued by Southampton University Center for Risk Research titled "Directing risk management in organizations". What is noteworthy about this new and radical risk management guidance is it explicitly recognizes that little empirical research has been done to assess the true effectiveness of different ERM methods. The harsh truth is that over the past 20 years tens of thousands of expensive ERM efforts, including those using COSO ERM 2004, have failed badly resulting in trillions of dollars of damage to stakeholders that could have been prevented. An excerpt from page 4 of the Southampton guidance is included below:

Those overseeing risk management often receive advice from risk management specialists and are expected to be appropriately sceptical and challenging while still supportive of the goal of managing risk well. In doing this, they should understand that risk management is a difficult and controversial area. Experts do not yet agree on many important points such as the meaning of the word "risk", the scope of risk management, and the value of commonly used and recommended techniques. Very few initiatives to improve risk management are evaluated scientifically and general guidance and regulations on risk management by organizations are not yet evidence based. ***The evidence that does exist shows that some familiar methods have serious logical flaws, are confusing to users, and produce poor results****. Proposals for developing risk management within an organization may not lead to initiatives that are effective and worthwhile, even if they have been designed by experts and are consistent with leading guidance and applicable regulations.*

Recommendation: the full COSO ERM guidance document should have a short section, perhaps in the Appendix, that candidly discusses the extent of real implementation of the COSO ERM 2004 guidance between 2004 and 2016; identifies areas where efforts to implement the COSO ERM 2004 guidance and ERM generally have been identified by various expert 2008 financial crisis post-mortem inquiries as sub-optimal; and outlines what has been done in this draft release to address the areas of ERM implementation now seen by regulators and other experts as needing improvement. In particular, it would be very helpful if the ED summarized specific areas/elements of status quo approaches to ERM identified by groups like the Financial Stability Board, Senior Supervisors Group, and Group of Thirty as major weaknesses that significantly contributed to the 2008 global financial crisis and outline how the new guidance addresses them.

Concern #2 – STRADDLING TWO CONFLICTING ERM PARADIGMS – the June ED is to be complimented on its heavy and consistent focus on the need to link ERM directly to strategy and objectives. Unfortunately, it appears to me that the exposure draft is attempting to straddle and maintain two competing ERM paradigms – the existing "risk centric" ERM paradigm on the one hand; and promoting the need for a new and better "objective centric" ERM paradigm on the other. A small sample of the ED's emphasis on the premise that risk management should be fundamentally about managing uncertainty linked to the achievement of strategic and business objectives is included below.

An "uncertainty" is generally understood to be something not completely known, or the condition of not being sure of something. Risk involves uncertainty and affects an organization's ability to achieve its strategy and business objectives. Therefore, one challenge for management is determining how much uncertainty—and therefore how much risk—the organization is prepared and able to accept. Effective enterprise risk management allows management to balance exposure against opportunity, with the goal of enhancing capabilities to create, preserve, and ultimately realize value. (p. 9/132)

"Strategy" refers to an organization's plan to achieve its mission and vision, and to apply its core values. A well-defined strategy drives the efficient allocation of resources and effective decision-making. It also provides a road map for establishing business objectives. (P.10/132

In business uncertainty exists whenever an entity sets out to achieve future strategies and business objectives. In this context, risk is defined as: The possibility that events will occur and affect the achievement of strategy and business objectives. (p. 14/132)

Enterprise risk management is integral to achieving strategy and business objectives. Well-designed enterprise risk management practices provide management and the board of directors with a reasonable expectation that they can achieve the overall strategy and business objectives of the entity. Having a reasonable expectation means that the amount of uncertainty of achieving strategy and business objectives is appropriate for that entity, recognizing that no one can predict risk with precision. (p.16/132)

In assessing risk to executing the strategy, management specifies business objectives—such as financial performance, customer satisfaction, learning and growth, and compliance—and assigns these to different parts of the entity. An organization should have a means to reliably provide to the entity's stakeholders a reasonable expectation that it is able to manage risk associated with the strategy and business objectives to an acceptable level. (p. 30/132)

207. The organization develops business objectives that are measurable or observable, attainable, and relevant. Business objectives provide the link to practices within the entity to support the achievement of the strategy. For example, business objectives may relate to:
• Financial performance: Maintain profitable operations for all businesses.
• Customer aspirations: Establish customer care centers in convenient locations for customers to access.
• Operational excellence: Negotiate competitive labor contracts to attract and retain employees.
• Compliance obligations: Comply with applicable health and safety laws on all work sites.
• Efficiency gains: Operate in an energy-efficient environment.
• Innovation leadership: Lead innovation in the market with frequent new product launches.

208. Business objectives may cascade throughout the entity (divisions, operating units, functions) or be applied selectively. Cascading objectives become more detailed as they are applied progressively from the top of the entity down. For example, financial performance objectives are cascaded from divisional targets to individual

operating units. Alternatively, many business objectives will be specific to an operational dimension, geography, product, or service. (p.60/132)

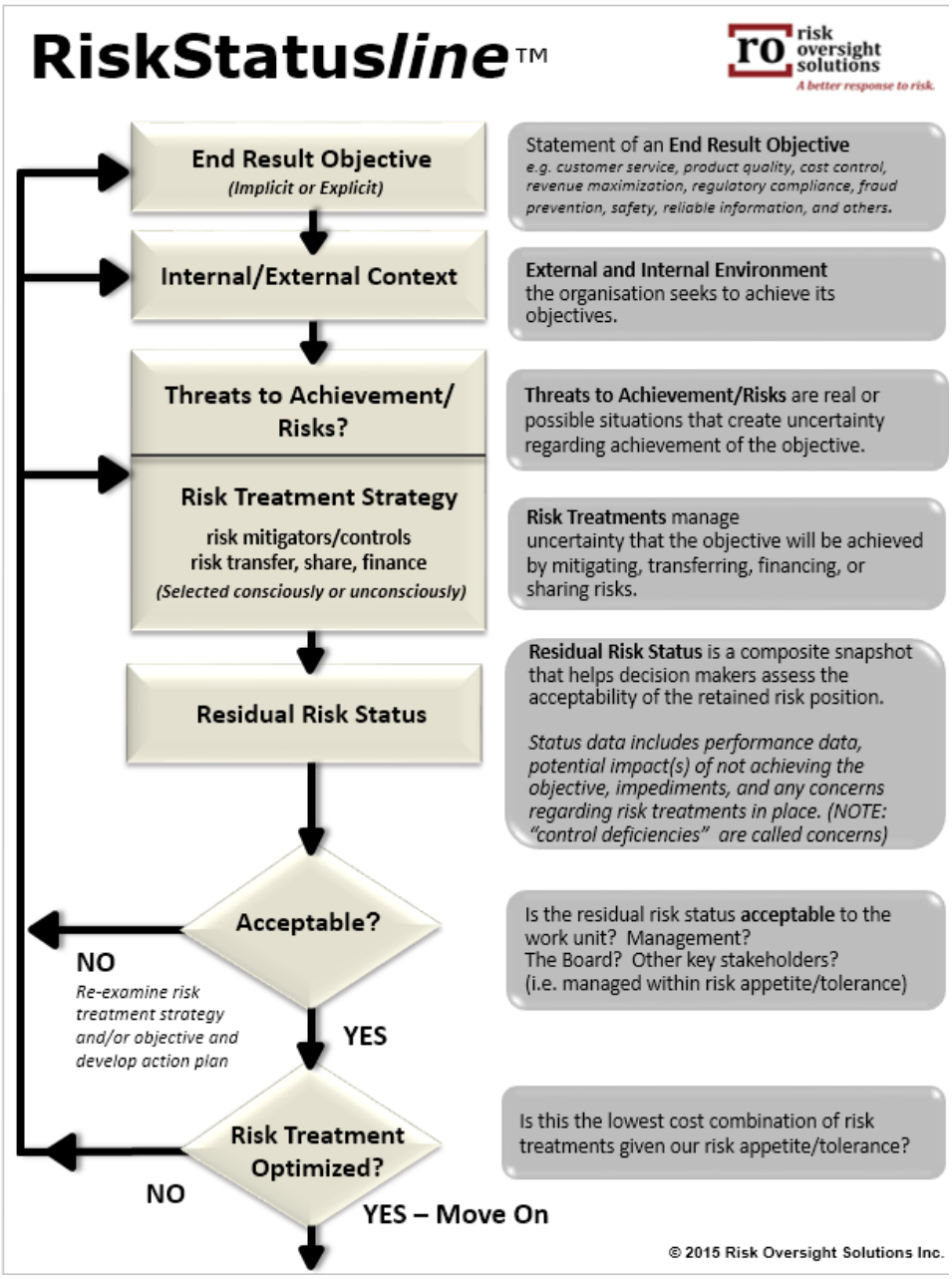
234. Creating, preserving, and realizing an entity's value is further enabled by identifying, assessing, and responding to risk that may impact the achievement of the entity's strategy and business objectives (p.68/132)

Unfortunately, large sections of the June 2016 ED still promote methods that use risk registers as a foundation for ERM; promote the use of heat maps that separate risks from the strategy/objectives they relate; promote the development and reporting of risk profiles that separate risks from the strategy/objectives they relate; promote risk analysis that looks at risks to strategy/objectives in isolation of other linked risks, not collectively in terms of their composite impact on the achievement of objectives. I can find no indication in the ED that suggests that the authors/COSO believe that an organized attempt should be made to ensure that key value creation and value preservation objectives are documented; and decisions made on which of those strategic and business objectives warrant the cost of formal risk management methods. Nor can I find any guidance on how organizations should decide the level of risk assessment rigour warranted on specific and key strategic value creation and value preservation objectives. As an outside observer, it almost appears that the ED authors are divided in two competing groups – one camp that support a new and better objective-centric/performance linked approach to ERM; and another camp that are still strongly wed to the risk-centric approach that is the dominant and sub-optimal ERM paradigm in the world today - a paradigm that uses risk registers as a foundation for ERM supplemented by risk heat maps, risk profiles, and other risk-centric tools.

Recommendation: The ED should recognize that the current dominant ERM paradigm in use in the world today is risk centric; generally uses risk registers as a foundation; focuses on risks in isolation to objectives; does not link performance being achieved on specific objectives to the risks and risk treatments in place; and most importantly, does not relentlessly emphasize that the primary purpose of formal risk management should be to manage uncertainty linked to the achievement of strategy and objectives. It should describe to readers the key elements of a true objective-centric ERM approach, an approach that starts with the simple step of documenting an organizations top strategic objectives and value preservation objectives key to long term value creation and value preservation, and then makes conscious decisions on which of those objectives warrant the cost of formal risk management. Once the strategic and value creation/value preservation objectives that warrant the cost of formal risk assessment are agreed by senior management and the board and documented in an "OBJECTIVES REGISTER", decisions should be made on who will be responsible for assessing and reporting upwards to senior management and the board on the state of residual/retained risk; the level of risk assessment rigour senior management and the board think is appropriate in light of cost/benefit considerations; and which group/person, if any, will provide independent assurance that the risk assessment process and representations on status to the board are reliable. The OBJECTIVES REGISTER should be regularly revisited and objectives added and deleted as priorities and risk governance resources change. Pro-forma objectives being considered for new strategies can be included in the REGISTER.

In an objective-centric ERM approach internal audit should be tasked with reporting on the reliability of the overall ERM framework and the reliability of the consolidated report on risk

status linked to key value creation and value preservation objectives the board receives from senior management. More details on objective-centric ERM approaches that use an OBJECTIVES REGISTER as a foundation can be found in the list of supplemental readings at the end of this response. An illustration of an objective-centric/ISO 31000 compliant risk assessment approach that encompasses many of the risk assessment elements covered in the June 2016 ED is shown below. This assessment approach is consistent with a large percentage of the guidance in the exposure draft. The words "risk treatment" in the diagram can be replaced with "risk response" without any change in meaning. The concept of painting a picture of "residual risk status" for decision makers to decide if it is within an entity's risk appetite/tolerance and the focus on risk treatment "optimization" are unique to this approach.



Concern #3 – CONFLICTING GUIDANCE ON ERM AND INTERNAL CONTROL – the ED makes references in a few places to the linkages between the June 2016 ERM ED and the COSO 2013 Integrated Control Framework. As someone who has expert knowledge of the evolution of internal control models and the evolution of ERM I am not persuaded that the current attempt in the ED to distinguish what is, in essence, two very different ways to accomplish the same goal is useful or successful. Page 10 of 132 of the main ED states:

Internal Control
11. "Internal control" is best described as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance that objectives relating to operations, compliance, and reporting will be achieved. Internal control helps the organization to understand the risks to achieving those objectives and how to manage risks to an acceptable level. Having a system of internal control allows management to stay focused on the entity's operations and the pursuit of its performance targets while operating within the parameters of relevant laws and regulations.

12. COSO's publication Internal Control—Integrated Framework is intended to help management better manage the risks associated with achieving their objectives, and to enable a board of directors to oversee internal control. To avoid redundancy, some aspects of internal control that are common to both this publication and Internal Control—Integrated Framework have not been repeated here (e.g., assessment of fraud risk relating to financial reporting objectives, control activities relating to compliance objectives, the need to conduct ongoing and separate evaluations relating to operations objectives). However, other aspects of internal control are further developed in the Framework 2 section (e.g., governance aspects of enterprise risk management). Please review Internal Control— Integrated Framework3 as part of applying the Framework in this publication.

The ED communicates repeatedly that the purpose of formal risk management is to manage uncertainty related to the achievement of objectives, including, presumably, core value preservation objectives like publishing reliable financial statements, complying with the law, cyber security, and others to a level of retained risk acceptable to senior management and boards. Unfortunately, initiatives like SOX 404 in the U.S. ask that senior management (CEOs and CFOs) and external auditors form binary opinions on whether they think "internal controls" are "effective". In risk speak, this is akin to asking an auditor if they like the level of residual risk being accepted by management. The term "internal control" is not covered in the ED as a way of responding/treating specific risks to objectives, but the term "Risk responses" is introduced and explained. Internal controls are only one form of risk response. They are primarily intended to work on reducing likelihood and/or consequences of one or more risks. There are four other primary risk treatment/response methods.

I have difficulty understanding why the authors of this guidance and COSO are reluctant to recommend that the risk identification and assessment methods being described in this draft guidance should be applied to all objectives, including reliable financial statements; safeguarding

confidential information against theft, alteration, loss; complying with laws, and other areas currently seen as being in the "internal control" domain, but not the ERM domain. That decision condemns the world to continued maintenance of two parallel and expensive frameworks – an ERM framework as well as a conflicting "internal control" framework.

Recommendation: This ED should do a better job explaining why COSO supports maintaining two competing and conflicting paradigms – one that says that an effective ERM framework can manage uncertainty to the full range of objectives; and another that says auditors, both internal and external should still focus on doing direct report audits and opining on the "effectiveness of internal controls" without requiring a documented risk assessment be made by management on relevant objectives that auditors review and opine on. National regulators, particularly the SEC in the U.S., are perpetuating the problem caused by this disjoint by requiring, via current SOX 404 implementation rules, binary opinions on "control effectiveness" from management and external auditors, while at the same time indicating publicly listed companies should all implement effective risk management frameworks that focus on developing frameworks that assess the acceptability of residual risk. Why should companies be required by law to maintain two different taxonomies and approaches and provide boards and regulators with assurance on both – one being an ERM paradigm focused on ensuring management and the board are aware of the true state of retained risk linked to key objectives, and the other, arguably obsolete, internal control effectiveness paradigm that is usually applied to a small subset of the risk universe? It is both hugely expensive and counterproductive. More details on the solution we propose to the massive global burden caused by the current regulatory/COSO drive to maintain two parallel and competing assurance approaches can be found in my April 2015 article, Reinventing Internal Audit, and our 2011 article Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act. The article Reinventing Internal Audit was recently awarded the 2016 Outstanding Contributor award from the global Institute of Internal Auditors.

Concern #4 – LACK OF RECOGNITION AND INTEGRATION WITH ISO 31000 RISK MANAGEMENT STANDARD

I completed a word search on the primary 132 page COSO ED document for the words "ISO 31000". ISO 31000 2009 is the global risk management standard. The search indicated no matches were found. Since this COSO ERM guidance will, almost certainly, compete against ISO 31000 for global dominance as the global risk management standard; and surveys have consistently indicated that ISO 31000 has, at least to date, been more globally accepted as ERM guidance; I found this surprising. For those interested that want to better understand the evolution and differences in the two main ERM frameworks, a very good presentation that describes the global dominance of ISO 31000 from PwC South Africa can be found at http://g31000.org/wp-content/uploads/2014/08/G31000-PwC-presentation-on-COSO-ISO-at-the-IIA-SA-conference-11-Aug-2014.pdf. Another useful reference to gain insight on global acceptance of COSO ERM 2004 is a post from Norman Marks available at https://normanmarks.wordpress.com/2012/05/11/final-results-of-coso-vs-iso-risk-management-survey/. My analysis of the June 2016 COSO ERM draft is that it has moved closer to the

philosophies in ISO 31000 2009 in a number of important ways, but continues to have some significant differences in terms of taxonomy and emphasis.

Recommendation: Instead of ignoring the global dominance of ISO 31000 as the leading risk management standard and the practical need to help organizations decide which of the two approaches best meet their needs, I recommend that the COSO team add an appendix which describes the key differences between COSO ERM 2016/17 and ISO 31000 2009 and explains why the COSO development team and advisors chose the approach they selected in the final COSO ERM guidance. This should include identifying all major differences in specific definitions and overall guidance approach between ISO 31000 and COSO ERM, including the definition of the word "risk", the use of the term "severity" vs "consequences", the use of "risk responses" vs "risk treatments" and many others. The increased focus in the ED on the importance of understanding internal and external context brings COSO ERM closer to ISO 31000. I believe the heavy emphasis in the ED on the need to link ERM to strategy and business objectives has the potential to make COSO ERM 2016/2017 the more effective framework relative to ISO 31000 2009.

Concern #5 – THE ROLE OF INTERNAL AUDIT – the ED describes a vague role for internal audit that is captured below. Internal audit can play a key role in effective ERM, but needs to fundamentally change its current role and methods in the majority of organizations around the world if effective risk governance and healthy risk cultures are primary goals.

Third Line: Assurance Functions
419. Assurance functions, most commonly internal audit, often provide the last line of accountability by performing audits or reviews of enterprise risk management practices, identifying issues and improvement opportunities, making recommendations, and keeping the board and executive management up-to-date on matters requiring resolution. Two factors distinguish the last line of accountability from the others: the high level of independence and objectivity (enabled by direct reporting to the board), and the authority to evaluate and make recommendations to management on the design and operating effectiveness of the entity overall.

At the current time the vast majority of internal audit departments complete direct report audits (audits where the primary assessor is internal audit not management) on a small percentage of the risk universe each year with a focus on opining on the "effectiveness" of internal control. These opinions are often subjective views that are, in essence, whether the auditors think the current retained/residual risk is, or is not, within what they think is senior management and the board's risk appetite. Research surveys confirm that only a small percentage of internal auditors focus on their organization's top strategic and value creation objectives. Most do not complete assessments that identify and assess all key risks to an objective or objectives being assessed or identify and consider the full range of risk responses/treatments. Very few internal audit departments provide boards with a composite picture of the retained/residual risks linked to the organization's top value creation and value preservation objectives. The approach used by many internal auditors is often not the type of structured risk assessment approach described in the COSO ERM exposure draft. The current internal audit paradigm impedes rather than supports effective risk management

practices and healthy risk culture. More details on the problems caused by the current status quo approach to internal audit are available in my April 2015 article "Reinventing Internal Audit".

Recommendation: Include a full section headed "IMPLICATIONS FOR INTERNAL AUDIT, SAFETY, ENVIRONMENT, INSURANCE AND OTHER ASSURANCE SPECIALISTS". This should describe how the role of these groups should/would change in organizations that implement the objective centric and management driven ERM approach being recommended in this new guidance. I believe that the role of internal audit should be to focus on quality assuring the risk assessment and management framework maintained by management; providing feedback and coaching to management groups; and providing an overall report on the reliability and effectiveness of the organization's risk management processes, including the reliability of the consolidated retained risk status reports prepared for the board. Insurance departments need to significantly increase their reliance on the organization's ERM framework to analyze the need for insurance and other risk sharing/transfer responses. Risk assessments done should include relevant details on insurance and other vehicles to finance/share risks. Safety and Environment groups should use the same risk assessment methodology the rest of the company uses for its ERM framework.

SUPPLEMENTAL REFERENCES/SUPPORT:

1. Paradigm Paralysis in ERM and Internal Audit, Tim Leech and Lauren Hanlon, Ethical Boardroom, Summer 2016
2. Reinventing Internal Audit, Tim Leech, Internal Auditor, April 2015, 2016 IIA Outstanding Contributor Award
3. The Next Frontier for Boards: Oversight of Risk Culture, Parveen Gupta and Tim Leech, Conference Board Director Notes, June 2015
4. Three Lines of Defense versus Five Lines of Assurance: Elevating the Role of the CEO and Board, Tim Leech and Lauren Hanlon, The Handbook of Board Governance, Richard Leblanc, Wiley, June 2016
5. Preventing the Next Wave of Unreliable Financial Reporting: Why US Congress Should Amend Section 404 of the Sarbanes – Oxley Act, Tim Leech and Lauren Hanlon, International Journal of Disclosure and Governance, 2011

NOTE: These articles are readily available via the internet using a simple Google search command.