ro risk oversight
A better response to risk.

The High Cost of "ERM Herd Mentality"

By Tim J. Leech FCA CIA CRMA CFE

White Paper

March 2012

The High Cost of "ERM Herd Mentality"

Discussion Paper Abstract:

Enterprise Risk Management ("ERM") as a movement has been around for more than a decade. Unfortunately, a 2010 COSO survey disclosed that only limited progress has been made convincing senior management and boards that ERM is key to maximizing and safeguarding long term enterprise value, allocating expensive human and financial resources, or managing major risks to strategic and core business objectives. At the same time there is growing consensus that one of the root causes of the global financial crisis of 2008 was deficient risk management and oversight. The majority, if not all, of the organizations at the center of the 2008 global financial crisis had some form of ERM. In most cases their CEOs, CFOs and auditors had all previously certified they had effective internal control over financial reporting in accordance with the 1992 COSO Internal Control – Integrated Framework, including controls over risk assessment processes and valuation of the toxic investment products at the heart of the global crisis.

In light of the massive wave of corporate governance failures linked to the global financial crisis of 2008, regulators in the U.S., Canada, Europe and elsewhere now require public companies disclose specifics on how their boards of directors oversee the effectiveness of risk management. At the same time, institutional investors, credit rating agencies, and board of director associations are all calling for major improvements in risk management and oversight. The ERM movement is expected to accelerate exponentially globally as a result of these change drivers.

Mandating more of the same flawed risk and control management frameworks, tools and methodologies in their current form that have not delivered the results promised by their authors is not the right path. The global cost of failed risk and control management frameworks over the last five years totals in the trillions of dollars.

This paper suggests that the root of risk management failures is flawed risk and control management frameworks, methods and tools. These are referenced as "ERM HERD MENTALITY WRONG TURNS". Wrong turns are analyzed and specific recommendations for the SEC and security regulators around the world, ISO, COSO, the IIA, and others ("ERM HERD LEADERS") are proposed to lever greater benefits from the billions of dollars organizations are expected to spend in the next five years enhancing their risk management capabilities.

This white paper was written to encourage constructive discussion and debate. Feedback on this paper should be sent to Tim Leech, Managing Director Global Services, Risk Oversight Inc. via e-mail at tim.leech@riskoversight.ca.

The High Cost of "ERM Herd Mentality"

450 sheep jump to their deaths in Turkey

ISTANBUL, Turkey (AP) — First one sheep jumped to its death. Then stunned Turkish shepherds, who had left the herd to graze while they had breakfast, watched as nearly 1,500 others followed, each leaping off the same cliff, Turkish media reported.

In the end, 450 dead animals lay on top of one another in a billowy white pile, the *Aksam* newspaper said. Those who jumped later were saved as the pile got higher and the fall more cushioned, *Aksam* reported.

The estimated loss to families in the town of Gevas, located in Van province in eastern Turkey, tops $100,000, a significant amount of money in a country where average GDP per head is around $2,700.

Source: *http://www.usatoday.com/news/offbeat/2005-07-08-sheep-suicide_x.htm*

Since ERM emerged on the scene in the mid-1990's thousands of organizations around the world have implemented variants of ERM following the leadership of influential bodies, including the Australian/New Zealand Risk Management Standard 4360, ISO Risk Management standard 31000, Committee of Sponsoring Organizations ("COSO") 2004 ERM guidance in the U.S., the Combined Code and the Institute of Risk Management frameworks in the UK, bank regulators around the world, the Institute of Internal Auditors, consultants, software vendors, and early adopter ERM pioneers.

As a result of the 2008 global financial crisis, and the subsequent creation of new disclosure regulations in the U.S., Canada, the U.K. and elsewhere that require public disclosure of details on how boards oversee the effectiveness of risk management processes[1&2], the number of ERM adopters is expected to grow exponentially in the public and private sectors around the world. Unfortunately, many of the ERM frameworks in use today are sub-optimal at best and, in some high profile instances, played a significant role in the demise of whole organizations.

This article overviews emerging evidence that supports the view that a large percentage of ERM implementations to date have been sub-optimal at best, and fatally flawed at worst. It then chronicles some of the authoritative guidance and missteps at the root of what this article calls "ERM HERD MENTALITY". Sub-optimal, sometimes fatally flawed and dangerous methodologies at the root of ERM failures and sub-optimizations are referenced as "ERM HERD MENTALITY WRONG TURNS". Dangerous authoritative guidance from well-respected and well-intending sources ("ERM HERD LEADERS") linked to ERM HERD MENTALITY WRONG TURNS is identified to help others avoid following the same perilous route over the analogous ERM cliff. The article closes with specific recommendations for ERM HERD LEADERS to try and reduce the number of organizations adopting and implementing sub-optimal forms of ERM in the years ahead.

---

[1] *See Proxy Disclosure Enhancements, Release 339089, Security Exchange Commission, February 28, 2010 (http://www.sec.gov/rules/final/2009/33-9089.pdf)*

[2] *See CSA Staff Notice 58-306, 2010 Corporate Governance Disclosure Compliance Review, December 2, 2010 (http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20101203_58-306_2010-corp-gov-disclosure.htm)*

ERM HERD MENTALITY DEFINED

Definition[3]

The term herd mentality is the word herd, meaning "group of animals," and mentality, implying a certain frame of mind. However the most succinct definition would be: "how large numbers of people act in the same ways at the same times".

Herd behavior is distinguished from herd mentality because it applies to all animals, whereas the term mentality implies a uniquely human phenomenon. Herd mentality implies a fear-based reaction to peer pressure which makes individuals act in order to avoid feeling "left behind" from the group. Herd mentality is also sometimes known as "mob mentality".

ERM HERD MENTALITY, as used in this article, refers to the adoption of specific and sub-optimal ERM methods and tools promoted, or at least not challenged or empirically critiqued and validated, by authoritative bodies that influence the actions of hundreds of thousands of public and private sector organizations around the world. Many sceptical senior executives and members of boards of directors have sensed the dangers of following the ERM HERD and been reluctant to fully support ERM, often as a direct result of previous exposure to failed ERM attempts. HERD MENTALITY was a key factor in the 2008 global financial crisis.

ERM FAILURES AND SUB-OPTIMIZATIONS – COSTLY DENIAL & HEAD IN THE SAND BEHAVIOUR

Following the onset of the 2008 global financial crisis, a group of the world's most respected bank regulators called the "Senior Supervisors Group" ("SSG"), including representatives from the U.S., Canada, Switzerland, the U.K, Netherlands, Japan, France, and Spain, began to study the events and circumstances leading up to the crisis to identify root causes and corrective actions needed going forward. In a seminal and tremendously insightful report that has influenced bank regulators around the world SSG summarized their key conclusions:

In the attached report, we identify various other deficiencies in the governance, firm management, risk management, and internal control programs that contributed to, or were revealed by, the financial and banking crisis of 2008. Our report highlights a number of areas of weakness that require further work by the firms to address, including the following (in addition to the liquidity risk management issues described above):

- *the failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm;*
- *compensation programs that conflicted with the control objectives of the firm;*

[3] *Wikipedia, (http://en.wikipedia.org/wiki/Herd_mentality)*

- *inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement; and*
- *institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel.*[4]

When the SSG findings are analyzed and synthesized they point to major and, in some cases, fatal flaws in the risk management and risk oversight frameworks in place in some of the largest, and previously most respected, financial institutions in the world.

What is not stressed in the SSG report is that virtually all of the organizations they reviewed as part of their study would have claimed prior to the crisis to have effective enterprise risk management practices; and all would have spent tens of millions, even hundreds of millions of dollars implementing and maintaining various forms of ERM; and funding external audits, internal control and assurance groups including internal audit, operational risk management, regulatory compliance groups, and others. Unfortunately, likely as a result of a lack of mandate and/or resources or politics, the SSG reports on the 2008 global financial crisis do not attempt to probe or understand the deeper root causes that would help explain why the serious flaws they identified existed in scores of high profile and respected organizations.

What is also not identified by the SSG is that, as a result of the enactment of section 404 of the Sarbanes-Oxley Act ("SOX") in the U.S., virtually all of the organizations they reviewed following the 2008 global financial crisis were certified by their CEOs, CFOs and external auditors as having "effective" internal control frameworks over financial reporting in accordance with the 1992 Committee of Sponsoring Organizations of the Treadway Commission ("COSO") Internal Control - Integrated Framework ("COSO 92")[5]. The financial statements of those organizations included hundreds of billions of dollars of overstated assets.

The SOX 404 "illusory assurance" debacle continues to this day. MF Global, one of the newest gigantic corporate governance debacles, an organization where over a billion dollars of depositors' monies has been reported missing, was certified as having effective internal control in accordance with COSO 92 by their CEO, CFO, and their external auditors, PwC, as recently as March 10, 2010. The board of MF Global, quite reasonably, would have relied on PwC's certification of the effectiveness of MF Global's accounting control framework when forming their own opinion on internal control effectiveness. An excerpt from the MF Global March 31, 2010 10K report follows:

> *Management conducted an assessment of the effectiveness of the Company's internal control over financial reporting as of March 31, 2010* ***based on the framework established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission.*** *Based on this assessment, management has determined that the Company's internal*

---

[4] *Source: Risk Management Lessons from the Global Banking Crisis of 2008, October 21, 2009, Senior Supervisors Group, http://www.sec.gov/news/press/2009/report102109.pdf*

[5] *Note: "effective" is defined by the SEC as capable of reasonably preventing a single material reporting error*

control over financial reporting as of March 31, 2010 was effective and that there were no material weaknesses in the Company's internal control over financial reporting as of that date.

The Company's internal control over financial reporting as of March 31, 2010 has been audited by PricewaterhouseCoopers LLP, an independent registered public accounting firm, as stated in their report included within, which expresses an unqualified opinion on the effectiveness of the Company's internal control over financial reporting as of March 31, 2010.[6]

It is important to note that PwC should not be singled out or chastised for their apparently flawed opinion on internal control effectiveness at MF Global using the COSO 92 framework. The wrong opinions from the CEO, CFO and PwC on internal controls effectiveness at MF Global reportedly linked to over a billion dollars in unaccounted for client funds are not in any way an isolated incident. Thousands of corporations that have suffered crippling corporate governance failures and were forced to reissue financial statements over the past decade were previously certified by their senior management and external audit firms as having effective internal controls over financial reporting in accordance with COSO 92.

Of even greater interest and even far-reaching consequence is that PwC was retained by COSO on a pro bono basis to be the primary authors of the exposure draft of the 2012 COSO control framework update, a 20 year anniversary update intended to improve the seriously dated 1992 framework originally authored by one of PwC's predecessors, Coopers & Lybrand. COSO 92 is a framework currently used by hundreds of thousands of public and private sector organizations around the world to assess the adequacy of accounting control effectiveness as a result of the Sarbanes-Oxley Act of 2002 and an a 2004 SEC decision.

The SEC requires that all U.S. listed public companies use what they deem a "suitable" internal control framework for external reporting on internal control effectiveness. The 1992 COSO Internal Control – Integrated Framework has emerged as the dominant framework the SEC has approved for use by SEC registrants. The 2012 COSO internal control framework update authored by PwC, issued in exposure draft form for comment in December 2011 and due for release sometime in 2012, will almost certainly be quickly approved by the SEC as "suitable" when finalized. COSO 2012 will then, again almost certainly, become the primary framework used to assess effectiveness of control and risk management over external reporting by major public companies around the globe – regardless of whether it actually works well as a tool to reach reliable conclusions on internal control and risk management effectiveness.

To date, the SEC in the U.S. has not publicly raised any concerns about the hundreds of seriously flawed internal control effectiveness opinions filed with them by public companies using COSO 92, a framework they have officially approved for use; nor have any class action lawsuits been launched alleging negligence on the part of CEOs, CFOs and external auditors forming those seriously flawed SOX 404 control effectiveness opinions. In essence, materially wrong opinions on internal control effectiveness have become a globally accepted business norm – a norm that is apparently accepted by the SEC, the PCAOB, and security regulators around the world.

[6] *Source: MF Global 10K for Y/E March 31, 2010, page 89 http://www.faqs.org/sec-filings/100528/MF-Global-Ltd_10-K/*

What is even more disconcerting than the dramatically and apparently wrong MF Global control effectiveness opinions and thousands like them, is that COSO, an organization comprised of the American Institute of Certified Accountants, Institute of Internal Auditors, Financial Executives Institute, Institute of Management Accountants and the American Accounting Association, in spite of having full knowledge of the massive opinion errors on control effectiveness being made by those using their dated 1992 control assessment framework, continues to refuse to invest much, if any, time or money to determine why CEOs, CFOs and external auditors of major companies have arrived at such seriously wrong opinions on control effectiveness. [7] There is no evidence that this type of research was done as part of the COSO 2012 update project; nor would it be appropriate for PwC as primary author of COSO 2012 and many incorrect SOX 404 control effectiveness opinions using COSO 92 to objectively undertake such research.

It is very important for readers to note at this juncture that the COSO 2004 Enterprise Risk Management – Integrated Framework ("COSO ERM 2004) is one of the two primary ERM guidance frameworks in the world today (COSO ERM 2004 and ISO 31000 2009). It is built entirely on a foundation comprised of the five control categories that make up the COSO 92 control framework used today around the world for SOX 404 internal control effectiveness opinions and, as a result of the decision of the COSO board, those same five categories will serve as the core foundation for COSO 2012 scheduled for release in 2012.[8]

ERM FAILURES AND SUB-OPTIMIZATIONS – A LARGE PERCENTAGE OF SENIOR EXECUTIVES AND BOARDS HAVE BEEN RELUCTANT TO FOLLOW THE ERM HERD BUT MAY BE FORCED TO BY REGULATORS

In 2010, to explore the extent that COSO was influencing the adoption of ERM, COSO commissioned an independent survey of major companies in the U.S.[9] A key finding of the survey was that there was widespread reluctance on the part of senior executives and boards to implement the COSO vision of ERM, and serious reservations about its ability to achieve the benefits promised by its authors and sponsoring body. The survey also provided a window on the enormous power of COSO to influence the thinking of U.S. corporations and major companies around the world. Excerpts from the Key Findings section of that report include:

- *The state of ERM appears to be relatively immature. Only 28 percent of respondents describe their current stage of ERM implementation as "systematic, robust and repeatable" with regular reporting to the board. Almost 60 percent of respondents say their risk tracking is mostly informal and ad hoc or only tracked within individual silos or categories as opposed to enterprise-wide.*

---

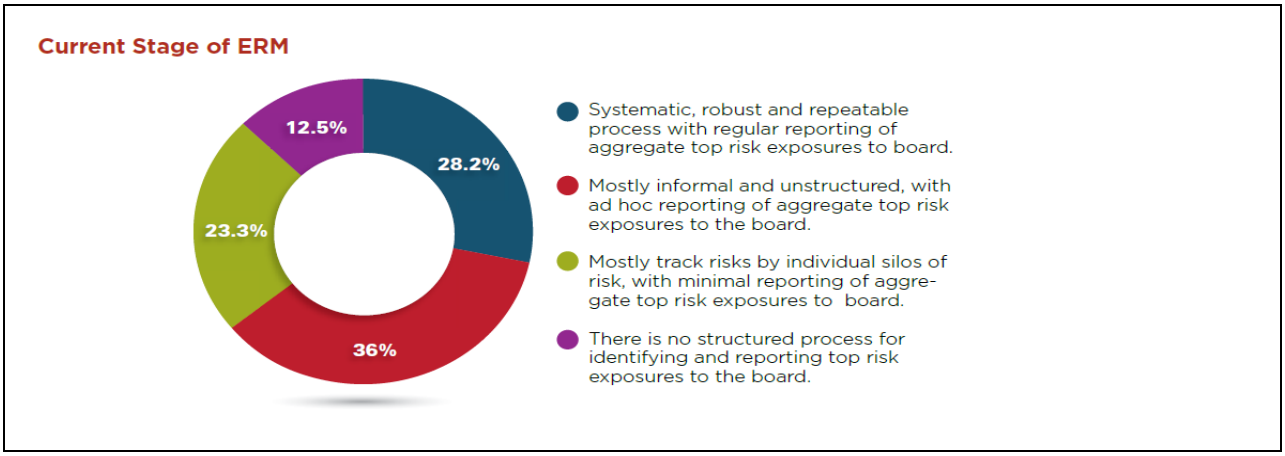
[7] Author's Note: If COSO and/or PwC, the authors of the 2012 COSO update, have completed an investigation to determine the root causes of materially wrong opinions on control effectiveness as part of the process used to develop the 2012 exposure draft they have not made it public.

[8] It is unclear at the time this paper was written if COSO will issue an update to its 2004 ERM Integrated Framework once COSO 2012 is released in final, or whether COSO 92 and COSO ERM 2004 frameworks will be withdrawn in favour of COSO 2012. Based on their references to the 2004 ERM framework it would not appear that they plan to drop or significantly change it.

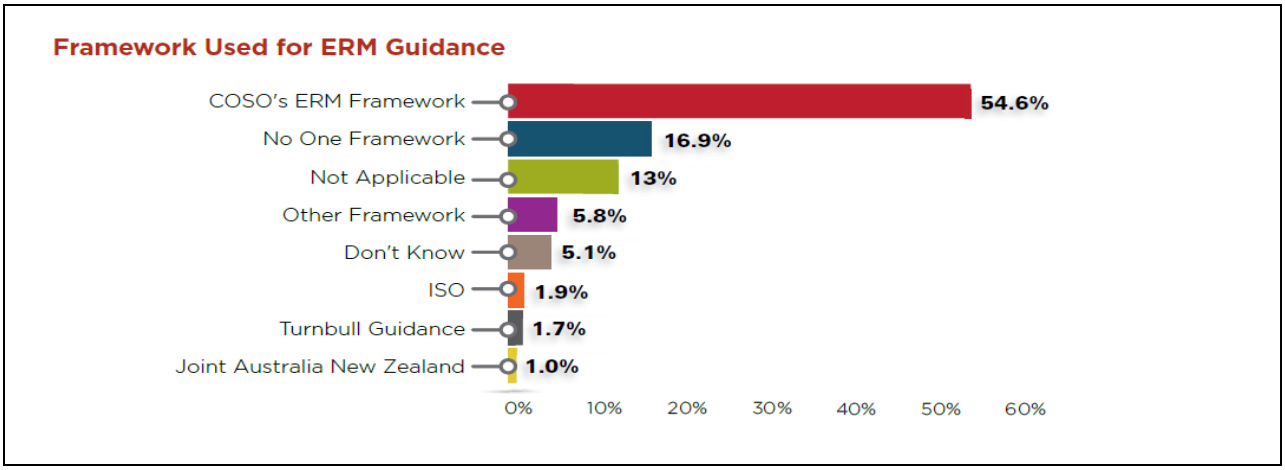
[9] COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework, Committee of Sponsoring Organizations of the Treadway Commission, Mark S. Beasley, Bruce C. Branson, Bonnie V. Hancock

- *There appears to be a notable level of dissatisfaction with how organizations are currently overseeing enterprise-wide risks. Almost half (42.4 percent) described their organization's level of functioning ERM processes as "very immature" or "somewhat mature." About a third (35 percent) admit that they are "Not at All Satisfied" or are "Minimally" satisfied with the nature and extent of reporting to senior executives of key risk indicators.*
- *Most believe that the COSO ERM Framework is theoretically sound, provides a common language for ERM that is widely accepted by organizations, and clearly describes key elements of a robust ERM process. There was some criticism that COSO's ERM Framework is overly theoretical. About a quarter (26.5 percent) responded significantly or "a great deal" to the perception that the COSO ERM Framework contains overly vague guidance.*

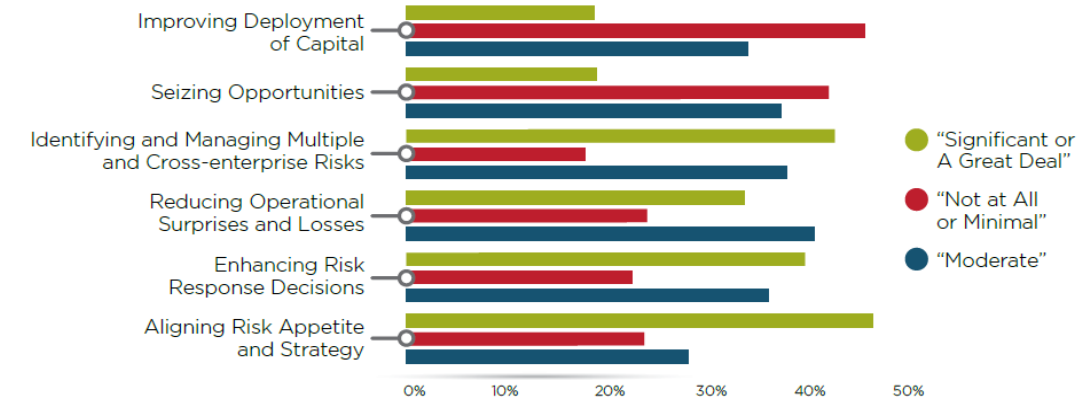
The table reproduced below shows that only 28.2% of companies surveyed claimed to have fully implemented a COSO vision of what constitutes ERM.



For those companies in the survey that were using a framework to implement ERM COSO ERM 2004 was the dominant choice by a large margin.



The survey also revealed that the majority of senior executives surveyed continue to be sceptical that implementing COSO ERM would bring the enormous business benefits promised in the COSO ERM guidance and elsewhere. The red bar indicates that almost 50% did not believe COSO ERM was capable of improving deployment of capital. (i.e. "not at all or minimal") Improved deployment of capital is often cited as one of the key benefits of an effective ERM framework.



WHY HAVE SENIOR EXECUTIVES AND BOARDS BEEN RELUCTANT IF ERM BENEFITS ARE HUGE?

Organizations including COSO, the Institute of Internal Auditors, ISO, Institute of Risk Management, leading consulting firms and many others have been promoting a long list of ERM benefits for over a decade now. A sample of the promised ERM benefits and their sources follows:

BENEFITS OF EFFECTIVE ERM PER ISO[10]

1. Increase the likelihood of achieving objectives;
2. Encourage proactive management;
3. Be aware of the need to identify and treat risks throughout the organization;
4. Improve the identification of opportunities and threats;
5. Comply with relevant legal and regulatory requirements and international norms;
6. Improve the mandatory and voluntary reporting;
7. Improve governance;
8. Improve stakeholder confidence and trust;
9. Establish a reliable basis for decision making and planning;

[10] *ISO 31000, Risk management- Principles and Guidelines p v-vi*

10. Improve controls;
11. Effectively allocate and use resources for risk treatment;
12. Improve operational effectiveness and efficiency;
13. Enhance health and safety performance, as well as environmental protection;
14. Improve loss and incident management;
15. Minimize losses;
16. Improve organizational learning; and
17. Improve organizational resilience.

BENEFITS OF EFFECTIVE ERM PER THE IIA[11]

- Organizational objectives support and align with the organization's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

BENEFITS OF EFFECTIVE ERM PER COSO[12]

- Aligning risk appetite and strategy
- Enhancing risk response decisions
- Reducing operational surprises and losses
- Identifying and managing multiple and cross-enterprise risks
- Seizing opportunities
- Improving deployment of capital

[11] *Assessing the Adequacy of Risk Management Using ISO 3100, December 2010, IIA.*
[12] *Enterprise Risk Management – Integrated Framework Executive Summary Framework, September 2004, The Committee of Sponsoring Organizations of the Treadway Commission, page3.*

TWO KEY QUESTIONS

1. Given that most, if not all of the companies at the root of the 2008 global financial crisis were using the 1992 COSO Internal Control Integrated Framework to assess the effectiveness of their financial reporting controls, and presumably internally for much broader purposes[13]; and all would have invested tens or even hundreds of millions of dollars to implement variations of ERM, often, according to COSO's 2010 ERM survey, using the 2004 COSO ERM Integrated Framework as guidance, why did things go so terribly wrong?

2. If ERM is truly capable of achieving all of the benefits listed above claimed by ISO, the IIA, COSO, and many others, why did such a large percentage of senior executives polled by COSO in 2010 indicate more than a decade after the global emergence of ERM that they don't buy many of the key ERM benefits claimed by COSO, the IIA, ISO, consultants, and software vendors around the world?

ERM HERD MENTALITY WRONG TURN #1 –ISO 31000 doesn't stress need for clear linkages to the objective(s) assessed, the impact of unclear/vague objectives, or the need for a composite assessment of uncertainty.

The core diagram in ISO 31000 risk management standard is reproduced below[14].

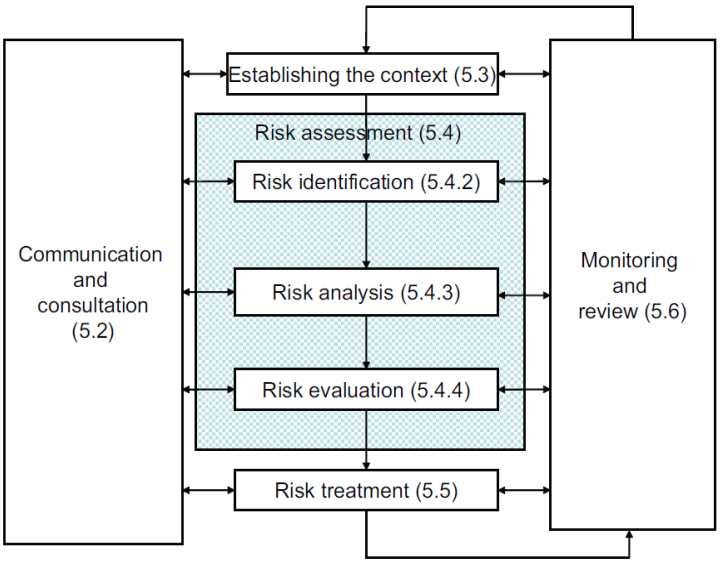


Figure 3 — Risk management process

[13] *Note: If organizations do not accept the validity and usefulness of COSO 1992 for purposes broader than reporting on internal control over financial reporting one has to question whether they believe it is truly useful or they have just been forced to use it by the SEC decision it is a "suitable" framework.*
[14] *ISO 31000, Risk Management Principles and Guidelines, First Edition, 2009-11-15, ISO*

ISO 31000 references the critical link between risks and objectives in its core definition of the word "risk":

1.1

risk

effect of uncertainty on objectives[15]

It references "objectives" again in the definition of what ISO 31000 calls "the context".

3.3.1.2
internal context
internal environment in which the organization seeks to achieve its objectives
NOTE Internal context can include:
— governance, organizational structure, roles and accountabilities;
— policies, objectives, and the strategies that are in place to achieve them;
— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
— information systems, information flows and decision making processes (both formal and informal);
— relationships with, and perceptions and values of internal stakeholders;
— the organization's culture;[16]

What ISO 31000 2009 does not do, and this is a major deficiency, is **stress to users via the core ISO 31000 process diagram and throughout the standard the need to start risk assessments with one or more clear end-result objectives and continuously maintain the connection between the risks identified and assessed and the related objective(s). ISO also does not call for a composite picture of the level and potential impact of uncertainty created by multiple risks relevant to one or more objectives being assessed**. (NOTE: This deficiency may be corrected in ISO 31000 guidance currently being developed which will be issued as ISO 31004:201X Risk management - Guidance for the implementation of ISO 31000[17])

In practice the absence of a clear ISO 31000 requirement to maintain clear linkages to the related objective(s) being assessed often results in ISO 3100 users not making the linkage between objective(s) and risks shown on heat maps, lists of risks in risk registers, reports on top risks to boards, and many other areas. The failure of organizations implementing ISO 31000 to stay true to the core ISO definition of "risk" being directly linked to specific objectives has far-reaching consequences.

---

[15] *Guide 73, Risk Management Vocabulary, ISO, First Edition 2009, page 1.*
[16] *Ibid, page 4.*
[17] Information on ISO 31004 provided by Kevin Knight, Chair of the ISO working group responsible for developing ISO 31000 guidance, on August 27, 2011. As of the date this paper was released in March 2012 the ISO 31004 project was shown as being at the "Preparatory stage" on the ISO website (http://www.iso.org/iso/standards_development/processes_and_procedures/stages_description/stages_table.htm#s20)

In addition to the need for there to be clear linkage to the objective(s) assessed, ISO 31000 doesn't put any emphasis on the need for clarity in the objectives being assessed. A simple illustration would be assessing the risks for two different, in ISO 31000 vernacular, "contexts":

CONTEXT #1 - I want to be west of here

Versus

CONTEXT #2 - I want to be at Latitude 43.44029 and Longitude -79.67595 by midnight tonight.

Risk assessments for these two objectives would look quite different.

The working group developing ISO 31000 implementation guidance for release in 2012 has been provided with a copy of this paper.

ERM HERD MENTALITY WRONG TURN #2 – Deciding that setting and communicating objectives isn't part of an integrated control framework.

COSO Enterprise Risk Management – Integrated Framework ("COSO ERM 2004") defines ERM as follows:

Enterprise risk management is a process, effected by an 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 its risk appetite, to provide assurance regarding achievement of entity objectives. [18]

So far, so good.

COSO ERM 2004 goes on to define one of the key components of an ERM integrated framework to be "Objective Setting". This is defined as:

Objective Setting – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.[19]

This is where the root of the ERM confusion and decoupling of objectives and risks starts. In the 1991 COSO internal control integrated framework exposure draft, a draft authored by Coopers & Lybrand, "Objectives" was one of 8 primary control categories in an integrated internal control framework. In the final COSO 92 release the COSO committee members concluded that:

[18] *Enterprise Risk Management- Integrated Framework, The Committee of Sponsoring Organizations of the Treadway Commission, page 4.*
[19] *Ibid, page 6.*

The "objectives" component has been eliminated as a separate component. The view expressed by some respondents that the establishment of objectives is part of the management process but is not part of internal control, was adopted. The final report recognizes this distinction, and discusses objective setting as a precondition to internal control.[20]

Following the release of the COSO 92 framework in the 1994/95 timeframe both the Canadian Criteria of Control Committee and the U.K. Cadbury framework authors both explicitly and publicly disagreed with the COSO decision that setting and communicating objectives was not a key part of an integrated internal control framework. Both countries included objective setting and communication as a full category in their respective frameworks[21]. To date, COSO has never publicly acknowledged the fact that both the Canadians and British rejected their 1992 decision that objective setting and communication is a precondition, not a key element of, an integrated control framework. They have also never publicly provided a rebuttal to the reasons for including objective setting and communication cited by the Canadians and British authors/sponsors.

It would seem that COSO 92 asks users to accept that objective setting is not part of an integrated control framework, but "Risk Assessment", one of five core COSO 92 categories, is a part of an integrated control framework, and that risk assessment includes using objectives, but apparently only if they exist.

In 2004, twelve years after the release of COSO 92, COSO reported that objective setting is a key element of **integrated risk management framework** but not of an **integrated control framework**. Again, it isn't clear in the 2004 COSO ERM framework what users of COSO 92 should do if clear objectives don't exist, or haven't been communicated to those that need to support them. This apparent disjoint between elements of an integrated control framework and integrated enterprise risk management framework was not explained in the COSO ERM 2004 document.

The COSO 2012 exposure draft update released in December 2011 again confirms that the five primary categories of control defined in COSO 92 (i.e. Control Environment, Risk Assessment, Control Activities, Information and Communication, & Monitoring Activities), categories that excluded the "Objectives" category included in the original COSO 91 exposure draft, will be retained and form the foundation for the 20 year anniversary update of COSO 92. The COSO 2012 exposure draft does state however, that:

A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories of operations, reporting, and compliance with sufficient clarity to be able to identify and assess risks to those objectives.[22]

It goes on to state in the new 17 principles of control that:

---

[20] *Internal Control – Integrated Framework, Framework Including Executive Summary September 1992, Committee of Sponsoring Organizations of the Treadway Commission.*

[21] *NOTE: both the Canadian CoCo and British Cadbury control frameworks are deemed "suitable" by the SEC for SOX 404 purposes but they have not, for obvious reasons, been studied or supported by the five COSO committee member organizations who in essence "own" COSO 92.*

[22] *Internal Control – Integrated Framework, Executive Summary, December 2011, Committee of Sponsoring Organizations of the Treadway Commission,page4.*

The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks related to objectives.[23]

So it would now appear that **setting and communicating objectives is one of the key "principles" of an integrated control framework** but we are asked by COSO to accept that it should still be viewed as a precondition to internal control and **not part of an integrated control framework.** The exposure draft reaffirms the confusion when it states:

Setting objectives is a prerequisite to internal control and a key part of the management process related to strategic planning. Management needs to understand the overall strategies set by the organization. As part of internal control, management specifies objectives that have been set so that risks to the achievement of those objectives can be identified and assessed. [24]

It isn't at all clear what an auditor is expected to do when reporting on the effectiveness of internal control in accordance with COSO 2012 if management has not actually specified and communicated clear objectives in one or more areas being evaluated. That type of situation would not appear to be a reportable control deficiency using COSO 1992, or the new 2012 COSO exposure draft framework, as defining and communicating objectives is not considered by the COSO authors to be a part of an integrated control framework.

ERM HERD MENTALITY WRONG TURN #3 – Focusing on risks - one-by-one

A large percentage of ERM work identifies risks and then assesses each risk separately in terms of various combinations of likelihood, consequence, velocity, key risk indicators, and other factors. What is often not done is identify, assess, and examine the impact of multiple risks in terms of their impact and potential impact on the objective's performance and level of uncertainty linked to the related objective or objectives being assessed. Very few ERM approaches used today form a composite view on the overall level of uncertainty of achieving the objective(s) being assessed, or the impact(s) to the organization of non-achievement in whole or in part of the objective(s).[25]

ERM HERD MENTALITY WRONG TURN #4 – Making "Risk Registers" King

In many ERM implementations a key goal is to create and maintain a "Risk Register". The risk registers created often put significant emphasis on identifying and reporting the top 10 risks or top 20 risks facing the organization. Many boards of directors are accustomed to this and sometimes request "Top Ten Risks" reports. What many risk registers fail to do is to identify the top end-result strategic and core business objectives where there is high uncertainty regarding their achievement, and the potential impact(s) on the organization if the objectives are not achieved. Few organizations in the world today

[23] *Ibid, page page 7.*
[24] *Internal Control – Integrated Framework, Framework, December 2011, Draft for Exposure, page 6.*
[25] *Note: in many reports on risks to senior executives and the board the related end-result business objective(s) are not articulated at all).*

provide a list of important business objectives that have high levels of uncertainty related to their achievement for senior management or boards of directors. (NOTE: Composite uncertainty reporting could include reporting to senior executives and the board the specific line items and note disclosures in financial statements that have the highest levels of uncertainty using a color coding system).

ERM HERD MENTALITY WRONG TURN #5 – Falling in Love with "Heat Maps"

As a result of the information most boards receive from their organization's ERM processes, more than a few directors associate ERM with what are called risk heat maps. These are often colour coded and position risks on likelihood and consequence axis usually using 3X3 or 5X5 grids. In some cases the authors attempt to show risks before "risk treatments" and after considering risk treatments, although this step is often blurred or omitted. What the diagrams lack is the ability to communicate which related business objectives have the highest uncertainty attached to them as a result of the existence of those risks. Some organizations simply plot risks using their X out of 3 or X out of 5 likelihood and consequence ratings. The result is that virtually certain likelihood risks with massive consequence are identified as "key risks" organizations should pay the most attention to (i.e. they have a numeric score of 25/25 or 9/9) while low likelihood/massive consequence risks are relegated to the bottom.

A December 2009 discussion paper titled ***A New Approach for Managing Operational Risk: Addressing the Issues Underlying the 2008 Global Financial Crisis***[26] sponsored by the Joint Risk Management Section of the Society of Actuaries, Canadian Institute of Actuaries, and Casualty Actuarial Society authored by Stamford Risk Analytics and Towers Watson raises a number of important concerns related to the dangerous elements of traditional heat map thinking. They suggest it should be considered a misnomer to call something that is a virtually certain likelihood a "risk" as there is little or no uncertainty. They suggest situations like this, while not unimportant, should be part of loss management not risk management. They also raise serious concerns with the practice of relegating low likelihood/high impact risks (risks assigned a 3/9 or 5/25) when numeric rating are used to low risk status on heat maps. Many major organizations in the world relegated the risk of a serious and widespread downturn in U.S. real estate valuations as a low likelihood/high consequence risk and, if it was explicitly identified and reported upwards at all, represented it on the bottom left quadrant of their risk heat maps. We all know how that decision turned out.

ERM HERD MENTALITY WRONG TURN #6 – Ignoring "Black Swans"

Following the 2008 global financial crisis, and closely linked to the concerns raised by December 2009 Societies of Actuaries paper referenced above, there has been a significant escalation in interest in the methods used to identify and manage risks considered to be low likelihood/massive consequence – the "Black Swans". Traditional heat maps and processes used to identify significant risks and develop "Top 10 Risks Lists" have often missed entirely or, if they were identified and documented, excluded this type of risk. Traditional risk identification and assessment methods that rely heavily on "brain storming" and

[26] *A New Approach for Managing Operational Risk, Society of Actuaries, Canadian Institute of Actuaries, Casualty Actuarial Section, OpRisk Advisory, Towers Perrin, December 2009, (http://www.soa.org/files/pdf/research-new-approach.pdf)*

experiential identification using historical data have frequently missed the "next big one around the corner" or excluded it from serious analysis when it was identified. Although a well constructed end result business objectives register has great potential to act as a completeness check when completing ERM work, few organizations in the world currently use end result business objectives registers as a foundation for their ERM framework. (NOTE: Unfortunately this is often because of a serious lack of clarity on end result objectives and who is responsible for the full range of end result objectives necessary for long term success)

ERM HERD MENTALITY WRONG TURN #7 – Focusing on "Controls"

A large percentage of ERM initiatives today focus on identifying "controls" linked to specific risks instead of identifying all relevant forms of "risk treatments"[27]. Many ERM approaches in use today don't even use the broader term "risk treatment". Risk treatments are intended to include the full range of mechanisms that mitigate risks including risk transfer/sharing/financing mechanisms including insurance and contractual terms – all mechanisms that impact on risk likelihood and/or consequence. Many of the ERM software products on the market fixate on documenting and testing "controls" instead of the full range of risk treatments. The fact that the SEC in the U.S. mandates the use of control-centric assessment frameworks for SOX 404 use, and does not allow the use of risk assessment frameworks like ISO 31000 or COSO ERM 2004 for reporting purposes, further compounds the problem.

ERM HERD MENTALITY WRONG TURN #8 – Mandating the use of a "control framework" not a "risk management framework" for SOX 404

When the SEC and PCAOB first drafted their regulations and guidance they elected to require opinions from CEOs, CFOs and external auditors using, what they deemed at the time, "suitable" control frameworks. The SEC indicated that they deemed COSO 92, the Canadian CoCo framework, and the UK Cadbury frameworks to be "suitable". They specified four criteria[28] that a framework had to meet to be deemed suitable by them. Unfortunately they have never disclosed how they concluded any of the frameworks they deemed "suitable" actually meet the four suitability criteria they specified.

The result has been that the virtually all U.S. listed public companies adopted process/control centric assessment methods to support CEO/CFO certifications on control effectiveness. Since SOX was adopted thousands of companies have published materially wrong financial statements that later required restatement that were certified by their CEOs, CFOs and external auditors as having effective internal control over financial reporting in conformance with the 1992 COSO internal control integrated framework. The March 2010 certification by MF Global's CEO, CFO, and its external auditor PwC

[27] Note: some frameworks including COSO ERM use the term "risk responses" instead of "risk treatments". Risk treatment is the term promoted for global use by IS0 31000, the global risk management standard.
[28] *COSO: Is "It" Fit for Purpose? Tim J. Leech, Governance Risk & Compliance Handbook, Wiley, Chapter3 http://www.leechgrc.com/pdf/kb-sps/COSO%20Is%20it%20Fit%20for%20Purpose-1.pdf 2008*

referenced earlier in this paper is only one of thousands of seriously wrong control effectiveness opinions investors and other stakeholders have relied on.[29]

Continuing the current practice of using a control framework for SOX 404 reporting will require companies use a risk management framework like ISO 31000 or COSO ERM 2004 for ERM work, and a control framework like COSO 92 or COSO 2012 for external financial reporting. In essence, financial control reporting becomes yet another risk management silo with its own vocabulary and methodology - a framework that is not consistent with all other ERM work done on every other facet of the organization's operations.

In 2011 a proposal to amend the Sarbanes-Oxley Act of 2002 was made to the SEC Chairman's office and a range of Congressional Committees supported by an article that appeared in the September 2011 on-line International Journal of Disclosure & Governance. The article calls on Congress to amend section 404 of the Sarbanes-Oxley Act and require opinions from CEOs, CFOs and external auditors on the question of whether they have "effective risk management processes over financial reporting", instead of the current requirement for opinions on whether they have effective internal control in accordance with COSO 92. [30] There has been no response to date from the SEC or any U.S. Congressional Committee.

ERM HERD MENTALITY WRONG TURN #9 – Using flawed and unproven "Risk Treatment" tools like COSO 92/COSO 2012

Control framework authors implicitly promise, or at least imply, that an organization that manifests the elements of the framework, all things equal, should outperform those organizations that don't manifest the elements, or don't manifest them to the same degree. COSO was the first major organization in the world to produce a control framework in 1991/92. In the 1994/95 time period, following the creation of the COSO Internal Control - Integrated Framework, Canada produced an integrated control framework called Criteria of Control ("CoCo") and the UK created one most generally called either the Turnbull or Cadbury framework.[31] These are the three control frameworks currently officially deemed to be "suitable" by the SEC for SOX 404 reporting. Papers have been published by the author of this paper that refute the SEC's claim that any of the three frameworks deemed "suitable" by the SEC actually meet SEC framework "suitability" criteria.[32]

---

[29] The author of this paper approached the SEC to determine whether they would accept the use of COSO ERM 2004 or ISO 31000 as a "suitable" framework and was told that only an SEC registrant could request another framework be added to the SEC "suitable framework" list.

[30] Preventing the next wave of unreliable financial reporting: Why US Congress should amend Section 404 of the Sarbanes-Oxley Act, Tim Leech, Lauren Leech, July 2011. (http://riskoversight.ca/wp-content/uploads/2011/10/PreventingTheNextWaveofUnreliableFinancialReportingWhyUSCongressShouldAmendSOX404LeechandLeech.pdf)

[31] AUTHOR NOTE: Most UK companies listed in the U.S. use COSO 92 for public reporting, primarily because of pressure from their external audit firms. The SEC does not provide details on which specific Cadbury or Turnbull product they are referencing.

[32] COSO: Is "IT" Fit For Purpose?, Governance Risk and Compliance Handbook, Wiley, Chapter 3, 2008 (http://www.leechgrc.com/pdf/kb-sps/COSO%20Is%20it%20Fit%20for%20Purpose-1.pdf)

Unfortunately, to date, no research has ever been done that validates the premise that organizations that manifest the attributes of any of these framework actually have better internal control than those that don't. Of equal interest, no effort has ever been undertaken to determine if COSO 92 is superior to CoCo or Cadbury, or more contemporary governance risk and compliance frameworks like the OCEG Red Book GRC Maturity Framework[33] , as a predictive tool for control effectiveness opinions.

Some of the most significant areas of COSO 92 identified as being particularly flawed cited in research done by the Institute of Management Accountants Finance GRC Research Center include the following:

- Defining and communicating objectives is not considered to be part of an integrated internal control framework including objectives related to financial statement, line disclosures and supplemental note reliability.
- Lack of emphasis on the critical importance of aligned reward/punishment systems and the huge risks played by misaligned reward/punishment systems.
- Lack of emphasis on the critical importance of measuring whether controls in use/place are actually resulting in more assurance and the desired objective(s) will be achieved.
- Lack of emphasis on the key role the board of directors should play overseeing the effectiveness of risk management processes.[34]

ERM HERD MENTALITY WRONG TURN #10 – Not practicing what you preach

Most people acknowledge that ERM as a discipline makes a lot of sense. In many ways it is a lot like flossing your teeth – there is a lot of support for the premise that it is a good thing to do, and very little published research that supports the premise you shouldn't do it.

Unfortunately, a very important risk assessment that doesn't appear to have received the attention it deserves by regulators around the world relates to whether ERM actually works. An illustration of what an ERM objective risk assessment should include as risks is shown below. Very little has been done to treat the risks shown.

Objective: Ensure ERM methods and tools used are producing the desired business benefits.

RISKS:

- Risk treatment tools and frameworks selected for use don't actually work.
- Don't know what specific business results/benefits are sought by the company from ERM.

[33] *OCEG Red Book (GRC Capability Model) http://www.oceg.org/view/RB2Project*
[34] *Accounting Control Assessment Standards: The Missing Piece in the Restatement Puzzle, Institute of Management Accountants, February 2008, (http://www.leechgrc.com/pdf/kb-sps/The%20Missing%20Piece%20in%20Restatement%20Puzzle.pdf)*

- Don't know if ERM is actually producing the desired results/benefits/don't measure success.
- Senior executives and boards are unwilling to use formal risk assessment methods and tools on really important business objectives like acquisitions and major investments as they don't accept it really adds value.
- Senior executives and boards refuse to use ERM as a core element of strategic planning and budgeting as they don't buy the premise that it will help.
- Authoritative groups, including the SEC in the U.S., CSA in Canada, and security regulators around the world still do not accept that ERM should be used for the objective of producing reliable external financial disclosures. (NOTE: The refusal of the SEC to accept ISO 31000 compliant assessment methods means two separate data/software frameworks must be maintained. One for ERM work and one for SOX 404 assessment work)

Risk Treatments????

This paper raises a number of questions linked to the risks identified in the box above. It's time organizations like COSO, the SEC, the PCAOB, IIA, and all organizations in the public and private sectors that have adopted, or are considering adopting, ERM give serious thought to the effectiveness of the "risk treatments" in place to treat these risks.

RECOMMENDATIONS FOR ERM HERD LEADERS – SEC, PCAOB & Security Regulators Globally

1. Change laws and regulations to require CEOs, CFOs, and external auditors to **report on the effectiveness of risk management processes** that support the objective of reliable external financial disclosures and **discontinue the current practice of requiring opinions on the effectiveness of internal control over financial reporting using COSO 92** or other "control" frameworks. This will allow full integration of SOX 404 work with ERM efforts.
2. If the decision is to continue to require and support opinions on internal control effectiveness using COSO 92 or COSO 2012 built on the same five 1992 COSO control categories, take steps to ensure users of the SOX section 404 information are aware of the historic errors rates on control effectiveness opinions by company, by business sector, and by external audit firm. At least then users would know that relying on control effectiveness opinions in their current form comes with high risk.
3. Create regulations to enable and fund research to determine the root causes of wrong audit opinions on financial statements and wrong opinions on the effectiveness of internal control/risk management processes that support them. Publish the results of this research to assist COSO, and other approved reporting framework authors, improve the reliability of their frameworks.

4. Require COSO consider the results of ongoing research on effectiveness opinions and update their framework at intervals of no more than every five years consistent with ISO practices.

RECOMMENDATIONS FOR ERM HERD LEADERS – COSO

1. Discontinue the practice of using major global audit firms that now issue opinions on internal control effectiveness and derive large fee revenues from low level control testing to author control and risk management frameworks that now serve as "Generally Accepted Control Criteria", and also serve as the foundation of what may soon become the world's generally accepted assurance framework. It would be inconceivable today that one of the big 4 firms would be selected to author FASB or International Accounting Standards. The fact that PwC provided an opinion on the effectiveness of internal controls at MF Global and all of the big four audit firms certified that internal control over financial reporting was effective at multiple firms at the root of the 2008 global financial crisis just prior to the global crisis, should be sufficient evidence that it is time to discontinue this practice.
2. Request that the SEC levy a risk and control framework user fee on all public companies using the COSO frameworks to form control effectiveness opinions in order to fund development and research and allow for the discontinuance of the current practice of using pro bono external audit firms to author COSO work products. Money should be specifically earmarked for independent "cause of failure" research on flawed control effectiveness opinion. The work done for COSO by the ERM Initiative team at the NC State University Poole College of Management shows enormous potential which could be significantly enhanced with the necessary funds.
3. Research the root cause reasons why thousands of CEOs, CFOs and external auditors have reached materially wrong opinions on internal control effectiveness using COSO 92 before releasing COSO 2012 in final, if at all. Ensure the new 2012 framework fully addresses all the key areas that are determined to be root causes of the internal control opinion errors.
4. Research why Canada and the UK both rejected the COSO decision in 1992 that setting and communicating objectives is not part of an integrated control framework. Revisit the decision that COSO 2012 will be built on the same 5 control categories used in COSO 92. These categories have not served the public or investors well and do not fully and visibly address many of the root causes of major corporate governance failures.
5. Use the results of the research called for above to create one framework - "COSO - Integrated Assurance Framework" that can be used to provide assurance on any dimension of organized activity in the public or private sectors. The focus of the new integrated ERM/Control framework should be helping organizations design optimal "risk treatments" to mitigate the significant risks organizations face at a reasonable costs to investors and other stakeholders.

RECOMMENDATIONS FOR ERM HERD LEADERS – IIA

1. Disclose a potential conflict of interest. Disclose to all IIA members that they should not expect fully impartial and objective advice or training from the IIA with respect to internal control or risk management/ERM frameworks as a result of the IIA's membership in COSO.
2. Ensure the new Certification in Risk Management Assurance ("CRMA") curriculum includes balanced coverage of ISO 31000, COSO ERM, and the ERM HERD MENTALITY WRONG TURNS issues identified in this paper.
3. Alert all IIA members that the decision of COSO in 1992 that defining and communicating objectives is not part of an integrated control framework is not consistent with decisions reached by Canadian or British control framework developers. Research and publish an IIA position paper on this specific issue independent of the COSO Committee.
4. Fund and complete research on the differences between and the strengths and weaknesses of "risk-centric" and "objective-centric" ERM and report results of that research to IIA members and consider the impact on the CRMA exam curriculum currently being developed.
5. Take a lead role as a member of COSO to support independent research to determine why thousands of CEOs, CFOs and external auditors have reached materially wrong conclusions on internal control effectiveness using COSO 92.
6. Recommend to other COSO members that COSO not issue the COSO 2012 internal control integrated framework in final and call on the International Federation of Accountants ("IFAC") to issue integrated financial statement risk assessment and risk treatment guidance. Just as there is a global move to international accounting standards there should be a parallel move to international accounting control standards.

RECOMMENDATIONS FOR ERM HERD LEADERS – ISO

1. Evaluate what changes should be made to the ISO 31000 risk management framework to ensure that users understand the importance of clear end result business objectives when completing risk assessments, and the need to maintain clear linkage between risk assessment work and the related end result business objectives.
2. Consider whether the focus of risk assessment work should be on forming a composite opinion on the level of uncertainty of achieving one or more specified objectives versus current practices of assessing risks one by one, creating risk registers, heat maps, and top ten risk lists. This should include whether boards and senior executives would be better served with lists of key potentially high impact end result business objectives with high uncertainty levels, including objectives related to the company's financial statements, versus the current practice of lists of top risks without direct linkage to objectives impacted.
3. Consider including a requirement in the next update to the ISO 31000 risk management framework and the new ISO 31004 risk management guidance that users monitor the composite uncertainty of achieving strategic and core business objectives at all stages of the risk

management process as part of the evaluation of the acceptability of residual risk status and in reports to the organization's board of directors.

RECOMMENDATIONS FOR ERM HERD LEADERS – Corporate ERM Sponsors

1. Take steps to understand the differences between "risk-centric" and "objective-centric" approaches to ERM to determine which approach is most likely to produce the best overall business benefits.
2. Independently assess whether COSO ERM 2004 or ISO 31000 2009 is best suited to meet long term business needs. This should include determining which framework is best suited for use by Internal Auditors to report to the board on the effectiveness of the organization's risk management processes pursuant to international professional practice standard section 2120, and the need for boards of directors to disclose to investors and the SEC what they currently do to oversee the effectiveness of the organization's risk management processes.
3. Consider the benefits of formally requesting a ruling from the SEC whether they will accept the global risk management standard, ISO 31000, as "suitable" for reporting on risk and control management as part of the company's annual financial disclosures process.

THE RISKS OF FOLLOWING THE ERM HERD

The opening story chronicling the story of the sheep that followed their leaders over a cliff to their death or grievous injury has, unfortunately, everything to do with the way organizations have implemented ERM to date. Many of the frameworks, methods and tools used have proven to be sub-optimal at best, potentially fatal at worst, and yet more organizations each week around the world opt to follow the same ERM implementation path as those before them.

The key reason for ERM sub-optimization and, in some cases, demise of whole organizations, is excessive reliance on influential and powerful ERM HERD leaders to choose the right path. Unfortunately, following leaders that have not sensed danger and apparently have a strong sense of infallibility is dangerous. The sheep analogy is most appropriate when combined with the famous words of Kenneth Blanchard:

"If you keep doing what you've always done - you'll keep getting what you've always gotten."[35]

It appears that one of the greatest risks in the corporate world today is, in fact, the way we approach managing risk. It's high time the world quit relying on untested theories on what it takes to truly get it right. Ironic, isn't it?

[35] *Words of Wisdom, http://spiritteaching.com/words%20of%20wisdom.html*

Tim J. Leech FCA CIA CRMA CFE is Managing Director Global Services at Risk Oversight Inc. ("RO") - www.riskoversight.ca. RO has offices in Calgary, Alberta and Oakville, Ontario and Macungie, Pennsylvania. He has over 25 years of ERM experience working with major public and private sector organizations around the world. Tim has been recognized for his contributions to the risk and control field with outstanding contribution awards from IIA Canada, the Association of Certified Fraud Examiners, and the Ontario Institute of Chartered Accountants. He can be reached at tim.leech@riskoversight.ca.

ABOUT RISK OVERSIGHT INC.

Risk Oversight Inc. was established in 2010 to help companies, directors, internal auditors and risk specialists meet new and emerging risk oversight expectations in the US and Canada. The company has offices in Calgary, Alberta, Oakville, Ontario, and Macungie, Pennsylvania. Tim Leech, RO's Managing Director Global Services and one of RO's founding partners, has more than 25 years global experience helping company boards, senior management/workgroups, internal auditors and other assurance specialists implement more cost effective risk management and risk oversight frameworks. Neil Bothwell, RO's Managing Director has many years of oil and gas experience and is a recognized expert in the area of Sarbanes-Oxley (SOX) 404/ Canadian National Instrument 52-109. Lauren Leech, Director Risk Services has over 10 years of global experience in internal and external audit, SOX 404/NI 52-109 and ERM technology. Parveen Gupta, RO's senior advisor and head of the Risk Oversight's Learning Systems division, is widely recognized as a thought leader and innovator in the area of risk and governance learning and training systems.

RO Services:

- **Board Risk Oversight Gap Assessments (using CICA, COSO and ICGN criteria)**
- **Board of Directors/Senior Management Risk Oversight Training Sessions**
- **Fractional Chief Audit Officer/Chief Risk Officer**
- **Risk Self-Assessment (RSA) Training and Implementation Support**
- **Contract Internal Audit/Risk Management Services**
- **NI 52-109/SOX 404 Support Services**
- **Enterprise-wide Anti-Fraud Risk Assessments**
- **Enterprise-wide Compliance Risk Assessments**
- **US Foreign Corrupt Practice Act (FCPA) and Canadian Corruption of Foreign Public Officials Act (CFPOA) Compliance Program Implementation Support or Assessments**
- **Support for Oil and Gas Internal Control Representations (EPAP in Alberta)**
- **Joint Venture/Contract Audits**
- **ERM Software Selection and Implementation Support**
- **Officer/Director Due Diligence Litigation Support**

CONTACT INFORMATION

Tim Leech FCA CIA CFE CCSA
tim.leech@riskoversight.ca
416 720 0392

Neil Bothwell CA CIA
neil.bothwell@riskoversight.ca
403 874 2769