Should boards and CEOs care about COSO ERM 2017?

By Tim J. Leech

Source: Conference Board December 2017 https://www.conference-board.org/blog/postdetail.cfm?post=6631

As globalization accelerates and the internet continues to explode the amount of data available, CEOs and board directors have responded by getting ever more selective deciding which new developments warrant their limited time and attention. The new Committee of Sponsoring Organizations of the Treadway Commission (COSO) guidance *Enterprise Risk Management: Integrating with Strategy and Performance* issued in the summer of 2017 is an example of a new development boards and CEOs globally should consider a top candidate for their limited time and attention.

This doesn't mean I am suggesting CEOs and boards read the long and windy 200 plus page report. They should simply demand that the person responsible for investor relations, if they have one, or the CFO if they don't, tell them what needs to be done to respond to what major institutional investors (i.e. BlackRock, Vanguard), International Corporate Governance Network (ICGN) members, and credit rating agencies are increasingly demanding. They want evidence that public company CEOs are defining top value creation and preservation objectives, and identifying and assessing risks to those objectives. Perhaps most importantly, they want those CEOs to provide evidence that the board of directors is effectively overseeing that process. [i]

To provide some context, COSO was created in 1985 to study causal factors that can lead to fraudulent financial reporting after a wave of major governance failures in the United States. Its first major work product, *Report of the National Commission on Fraudulent Financial Reporting,* was issued in October 1987. That report had relatively limited impact globally and, at least judging from subsequent events, didn't do a great job reducing fraudulent reporting. In response to a recommendation in the 1987 Treadway report, COSO issued *Internal Control: Integrated Framework* in 1992. Over the next decade this guidance also had limited impact on U.S. companies or their C-suites and boards. It simply didn't get their attention. A study by the Institute of Management Accountants published in 2006 indicates that the COSO 1992 internal control guidance prior to the Sarbanes-Oxley Act (SOX) had little to no effect on 69 percent of "management-types" in U.S. companies prior to SOX. (See Exhibit 1 below).

This all changed dramatically after the enactment of SOX in 2002, when the SEC decided that CEOs and CFOs of all companies listed on U.S. exchanges must annually report whether they have effective internal control over financial reporting. The SEC stated based on arguable criteria that the 1992 COSO internal control framework was a "suitable framework" to report against.

EXHIBIT 1

TABLE 16: Use of the COSO 1992 Framework Prior to SOX

by Company Managements

Response Scale	Q1: Extent to which COSO 1992 utilized by our company to manage its enterprise risk and controls		
	Overall Sample (N = 373)	**Internal Auditors (N = 146)**	**Management-types (N = 227)**
	% of Total	% of Total	% of Total
1. No Extent	37.8% (141)	45.9% (67)	32.6% (74)
2. Some Extent	31.4% (117)	30.1% (44)	32.2% (73)
3. Moderate Extent	13.9% (52)	11.6% (17)	15.4% (35)
4. Large Extent	11.3% (42)	7.5% (11)	13.7% (31)
5. Not Sure	5.6% (21)	4.8% (7)	6.2% (14)

Source: COSO 1992 Control Framework and Management Reporting on Internal Control over Financial Reporting: Survey and Analysis of Implementation Practices, Parveen Gupta, Institute of Management Accountants, 2006

The SEC decision to stipulate that COSO 1992 was a suitable framework to form internal control effectiveness opinions against spawned a whole new industry of SOX units, SOX compliance specialists and SOX software that still lives on today. It caused companies worldwide to spend literally trillions of dollars of shareholder money over the next 15 years to comply. The jury is still out whether current SOX section 404 regulations pass the cost/benefit test or, more importantly, have significantly improved reliability of financial statements. In my professional opinion current SEC SOX section 404 rules are still seriously sub-optimal, largely because of

serious deficiencies in the 1992 and 2013 COSO Internal Control Integrated Frameworks [ii]. Interested readers should see the endnotes of this post for more details.

Having been an outspoken critic of COSO's most important work products to date, the COSO Internal Control Integrated Framework and COSO ERM 2004, it has surprised many, including Institute of Internal Auditors CEO Richard Chambers and current COSO chair Bob Hirth that I have been aggressively promoting, in a largely positive way, COSO's newest work product, *Enterprise Risk Management: Integrating with Strategy and Performance.*

COSO's First Try at ERM in 2004 – A Big Setback for Value Adding ERM

Expanding its scope far beyond its original mandate of reducing the incidence of fraudulent reporting, COSO took its first crack at what is generally called Enterprise Risk Management in 2004. Unfortunately for the world and shareholders, the COSO authors, comprised mainly of accountants, were generally of the view that ERM should focus on building "risk registers" – a list of bad things that people in workshops and interviews conjure up when asked "what could go wrong?" and "risk heat maps" – colourful depictions of prioritized bad things that could go wrong. These risk registers and risk heat maps were, at least in part, driven by a relatively ineffective SEC proxy disclosure requirement still in place today that require companies publicly disclose a long laundry list of "risks" in annual reports, with no reference to which strategic objectives they could impact, or what the company is doing, in ISO/COSO parlance, to "treat" or "respond" to those risks. Hundreds of thousands of organizations worldwide heeded COSO's guidance and adopted "risk centric" forms of ERM.

COSO 1992 to 2004 – Suboptimal at best, dangerous at worst

To the surprise of many who have followed my articles over the past 30 years including a published IIA blog titled "**Clarifying COSO's Raison d'être – It's Time To Set Clear Objectives and Report On Progress"** that opened with:

My conclusion, for those that don't like reading long blogs, is that the current state of affairs at COSO constitutes, in SOX parlance, a material control weakness, and that this deficiency constitutes a risk of global proportions to investors and regulators around the world.[iii]

I have publicly and repeatedly published positive reviews on COSO ERM 2017 since it was issued in July of this year to update the seriously sub-optimal COSO ERM 2004.[iv]

COSO ERM 2017 – What's different/better?

Biggest difference #1 – ERM is about increasing certainty objectives will be achieved

COSO ERM 2017 guidance, unlike their risk centric first try at ERM guidance in 2004, tries hard to promote the simple and incredibly important premise that ERM should start with really important strategic objectives. Risk assessments should all be linked to objectives. It goes further and indicates that risk centric/risk list forms of ERM spawned by COSO ERM 2004 and

still used by a large percentage of organizations globally are the least integrated and value producing form of ERM.[v]

While COSO ERM 2017 doesn't directly come out and apologize for helping create the view that having an effective ERM framework means creating and maintaining risk registers/risk lists, it comes close. The diagram in Exhibit 2 below describes ERM from "Minimal integration" to "Full Integration". The inference is clear that maximum value is created by "full Integration", an objective centric form of ERM focused on top strategic objectives, and that "minimal integration" is achieved with risk centric/risk register-based ERM.

EXHIBIT 2

Figure 8.10 Portfolio View of Risk

In developing a view of risk, there are four levels in order of ascending level of integration (from minimal to maximum):

- *Minimal Integration—Risk View:* At the risk-centric view, the entity identifies and assesses discreet risks. The predominant focus is on the underlying risk event rather than the objective; for example, the risk of a breach impacting compliance of the entity with local regulations.
- *Limited Integration—Risk Category View:* This view uses information captured in the risk inventory view and organizes risks using categories or another classification scheme. Risk categories often reflect the entity's operating structure and inform roles and responsibilities. A compliance department, for example, will have responsibilities for helping the organization manage its compliance-related risks.
- *Partial Integration—Risk Profile View:* Adopting a more integrated view, an organization focuses on business objectives and the risks that align with those objectives (e.g., all objectives potentially impacted by compliance-related risks). Further, dependencies that may exist between business objectives are identified and considered. For example, an objective of enhancing operational excellence may be a prerequisite for strengthening the balance sheet and growing market share. This view relies on information used to create the risk-centric or risk-category view.
- *Full Integration—Portfolio View:* At this level, the focus shifts to the overall entity strategy and business objectives. Greater integration supports identifying, assessing, responding to, and reviewing risk at the appropriate levels for decision-making. Boards and management focus greater attention on the achievement of strategy while responsibility and management of business objectives and individual risks within the risk inventory cascade throughout the entity. Using the same example, the board reviews and challenges management on how the entity is enhancing its operational excellence including the management of compliance-related risks.

In developing the portfolio view, organizations may observe risks that:

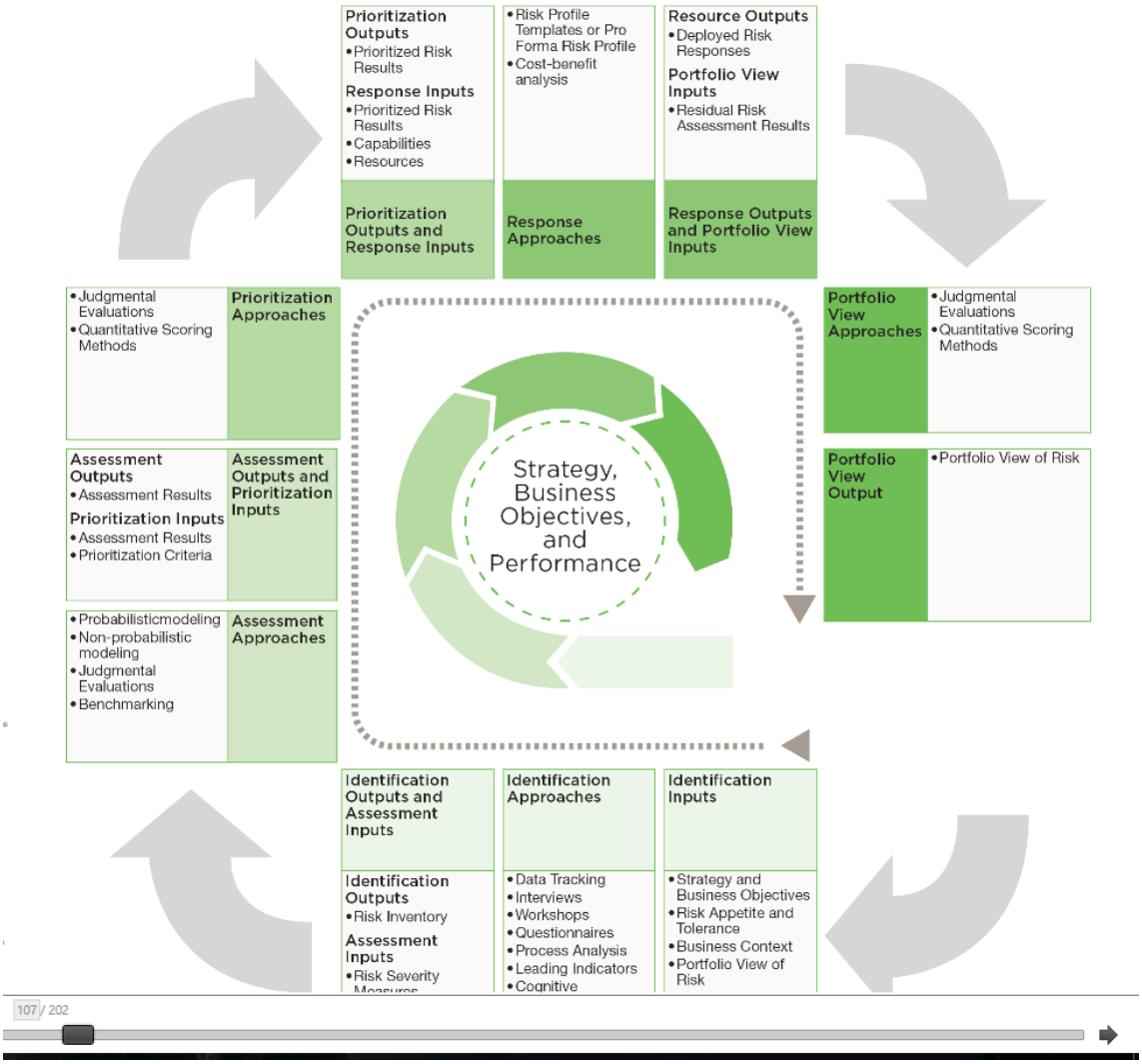
- Increase in severity as they are progressively consolidated to higher levels within the entity.
- Decrease in severity as they are progressively consolidated.
- Offset other risks by acting as natural hedges.

Biggest difference #2 – Start with important objectives and link to performance

While I think COSO could have done a better job in this area, the 2017 ERM guidance does, in Figure 8.1 shown below, promote the need to link formal risk assessments to important strategy,objectives and performance. [vi]

EXHIBIT 3

Figure 8.1: Linking Risk Assessment Processes, Inputs, Approaches, and Outputs



Why is linking risk assessments to top objectives and performance so important?

Truly effective ERM requires real and continuous involvement and ownership of boards, C-suites, and staff at all levels. Risk centric/risk register based approaches to ERM have failed in many respects to integrate formal risk assessment work products in to decision making linked

to the company's most important strategic, value creation and preservation objectives. Truly effective ERM should provide valuable information that helps boards, C-Suites and staff at all levels make better resource allocation decisions on key objectives. It should also provide valuable information to help gauge whether the current risk treatments/internal controls are actually working.

I learned many years ago in university in Psychology 101 that people repeat behaviors that they are rewarded for doing or punished for if they don't do. By requiring C-suites to define which objectives they think are important enough to warrant formal risk assessments, assigning "owner/sponsors" responsible for those objectives to assess and report on the acceptability of the current retained risk status and, most importantly, showing the link between risks, risk responses and current performance it sends a powerful message:

"The real purpose of ERM is to increase certainty you will achieve what you want and won't get what you don't want."

If the ERM approach you use or move to achieves this simple goal, it will motivate people at all levels, up to and including the board, to make better decisions on when formal risk assessments are worth doing; make decisions on the level of risk assessment rigor and resources each objective in the company's objective register warrants; decide which group, if any, should independently quality assure the assessments and report to the board on reliability; and how to best use the information produced to make better resource allocation decisions.

Thumbs up to COSO on COSO ERM 2017. It isn't perfect by a long stretch but it sends some very important messages missing or latent in COSO ERM 2004 that are key to increased global adoption of true integrated and value adding ERM.

Tim J. Leech FCPA FCA CIA CRMA is managing director at Risk Oversight Solutions Inc. headquartered in Oakville, Ontario, Canada and Sarasota, Florida. He is recognized globally as a thought leader and innovator in the risk and assurance fields. He has provided ERM and internal audit training and consulting services and technology to hundreds of thousands of professionals in public and private sector organizations in Canada, the United States, the United Kingdom, Europe, Australia, South America, Africa, the Middle East, and Asia. Tim`s April 2015 article, "Reinventing Internal Audit" received the 2016 Outstanding Contributor Award from IIA. Tim and Parveen Gupta's June 2015 *Director Notes* paper "The Next Frontier for Boards: Oversight of Risk Culture" was republished in the Harvard Law and Governance and Columbia law school blogs. Most recently, Tim's paper in the Spring Issue of Ethical Boardroom, "Focusing ERM and Internal Audit on What Really Matters: Long Term Value Creation and Preservation" has attracted global accolades and attention. Tim specializes in helping organizations implement objective centric ERM and internal audit to meet evolving risk oversight expectations and deliver substantially more value.

---

[i] See "Board Oversight of Long Term Value Creation and Preservation: What Needs to Change? Tim J. Leech, Conference Board Director Notes July 2017 for more details

[ii] See **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.

[iii] Clarifying COSO's Raison d'être – It's Time To Set Clear Objectives and Report On Progress, Tim Leech, Leech Talks Risk, IIA official blogs, February 2010**.**

[iv] For an example see "**COSO ERM 2017:** Why should boards around the world care about the 200-page US guidance? The answer might surprise you", Tim Leech, Ethical Boardroom, Autumn 2017

[v] See Enterprise Risk Management: Integrating with Strategy and Performance, COSO July 207, page 133/202.

[vi] Ibid