RESPONSE SUMMARY:

The COSO Board decided in 2010 to embark on a project to update the 1992 COSO Internal Control – Integrated Framework, but leave the core control categories and definition of internal control in the 1992 framework unchanged. The primary justification for the significant project scope limitation was that the 1992 COSO framework is broadly accepted and the core elements of the 92 framework are "timeless"[1]. This 2010 decision was heavily influenced by a survey COSO conducted that asked a relatively limited sample if they wanted incremental or major change.

This response challenges the core premise that COSO 1992 has been optimally effective for the primary tasks organizations use it for today, and the core assumption that the five core categories in the COSO control framework and definition of internal control should be considered "timeless".

We respectfully propose two transformational change recommendations for the COSO board to consider:

1. Suspend all work on COSO 2012 and request that the International Federation of Accountants ("IFAC") assume responsibility for creating a new international risk assessment and treatment standard.

2. Discontinue the current COSO practice of using external audit firms that opine on control effectiveness for SOX 404 representations as pro bono volunteers to drive COSO framework research and development. Request national security regulators around the world fund efforts through a fee charged to public companies to build and maintain a new global risk and assurance assessment and reporting standard that public companies would reference in public disclosures, much like references in financial statements to International Accounting Standards.

We believe that that a transformational change route is necessary to better meet stakeholder expectations and has enormous potential to produce significantly more societal benefits on a global basis.

[1] *"inasmuch as its core components are timeless", David Landsittel COSO Chairman, COSO Announces Project to Modernize Internal Control – Integrated Framework, COSO News Release, November 18, 2010.*

Submitted by: Tim Leech, Managing Director Global Services Risk Oversight Inc.
tim.leech@riskoversight.ca

Decision to Update COSO 1992 Using an Incremental Approach

When the COSO modernization project was announced on November 18, 2010 the COSO press release stated:

The Framework has been widely accepted as an internal control standard for organizations implementing and evaluating internal control related to operations, compliance, and financial reporting objectives, and more recently, internal control over financial reporting in compliance with the U.S. Sarbanes-Oxley Act of 2002 (SOX) and similar regulatory requirements in other countries.

Enhancements to the Framework are not intended to alter the core principles first developed in 1992, but rather facilitate more robust discussions of internal control. Certain concepts and guidance in the Framework will be refined to reflect the evolution of the operating environment, changed expectations of the regulators and other stakeholders.[2]

It was clear from this announcement that the COSO Board had concluded that the 1992 COSO Internal Control – Integrated Framework is still fundamentally sound and widely accepted and used. These fundamental beliefs and a limited sample survey supported a decision to embark on a limited incremental change strategy.

The 2010 COSO board decision to limit the scope of the update project at such an early stage can be viewed as a form of "framing", a condition described in COSO's most recent thought leadership paper as *"mental structures or perspectives that we use to determine the relevance or importance of information."*[3]

The COSO guidance on Enhanced Board Oversight goes on to state:

Different vistas or frames can lead to significantly different understandings or interpretations of a situation, and these different understandings and interpretations will affect behaviour and decision.

Although we recognize that it is very difficult to shift the opinion of a well-intending board of directors that has made a decision as core as the one above, our response requests that the COSO board revisit its decision to embark on limited and incremental improvement of the 1992 framework and consider two transformational recommendations on the best way forward.

In particular, we request the COSO board revisit the core underlying premises that we believe are at the root of the board's decision in 2010 to embark on incremental not transformational change. These are:

1. COSO 92 has been widely and voluntarily embraced by companies around the world as an effective business improvement framework.

[2] *COSO Announces Project to Modernize Internal Control – Integrated Framework, COSO News Release, November 18, 2010.*
[3] *Enhancing Board Oversight: Avoiding Judgment Traps and Biases, COSO, KPMG LLP, Steven Glover, Douglas Prawitt, March 2012*

2. COSO 92 has worked well for purposes of forming SOX 404 opinions on accounting control effectiveness.
3. There is no urgent need for a fundamentally different approach to risk and control management assurance.

We believe that the facts do not support the underlying assumptions that form the foundation for the COSO board's decision to limit 2012 update efforts to incremental improvement. In our opinion, transformational changes, not limited and incremental changes to the framework are necessary to better meet stakeholder expectations and needs going forward.

PREMISE #1 - COSO 92 has been widely and voluntarily embraced by companies around the world as an effective business improvement framework.

Prior to the decision of the SEC in 2004 to elevate the stature of COSO's 1992 Internal Control – Integrated Framework ("COSO 92") the real truth is that there had been only very limited voluntary acceptance and use of COSO 92 in the twelve years since its release. Table 16 drawn from a research study conducted by Professor Parveen Gupta on behalf of the Institute of Management Accountants is reproduced below. [4] Over 76% of Internal Auditors and close to 65% of Management were not using the framework at all, or were using it to a very limited extent.

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

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)

[4] *Internal Control COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices, Professor Parveen Gupta, Institute of Management Accountants, page 60.*

Following the decision of the SEC in 2004 to mandate COSO 92 for SOX 404 reporting on accounting control effectiveness use of COSO 92 for that purpose increased exponentially. Use of COSO 92 had become mandatory for U.S. listed public companies. Canada emulated the U.S. strategy to require reporting using COSO 92. At the time Boards of Directors, senior management of public companies, and the global external audit community were unwilling to even consider the merits of using the Canadian CoCo[5] or UK Cadbury[6] frameworks, the other two frameworks deemed "suitable" by the SEC. No attempt was made at the time, or since then, to empirically study which of the three internal control frameworks deemed "suitable" by the SEC is likely to produce the most reliable opinions on accounting internal control effectiveness.

In spite of the SEC mandating the use of COSO 92 by all U.S. listed companies, our belief is that few companies use COSO 92 in any serious tangible way today beyond their narrowly focused SOX 404 and external financial reporting work.

We see little tangible evidence in our work that organizations use COSO 92 in a tangible way to evaluate the "efficiency and effectiveness of operations", an important facet covered in the COSO 92 definition of internal control, or other areas like the effectiveness of an organization's other regulatory compliance frameworks. This conclusion is based on our own observations and interactions with risk and control professionals in companies around the globe. We are also not aware of any organization that actively uses COSO 92 in a tangible way to help auditors or management identify existing or potential "risk treatments" as part of their ERM initiatives. We believe that, while further research to determine the true use of COSO 92 today is necessary and warranted to determine the true extent of COSO 92 adoption, global adoption of COSO 92 has been primarily driven by the SEC decision in 2004 to deem it a "suitable" framework, not its inherent appeal to management as a useful business tool to evaluate and manage the full range of risks to all types of business objectives.

PREMISE #2 - COSO 92 has worked well for purposes of SOX 404 opinions on accounting control effectiveness.

Research done by the Institute of Management Accountants Finance GRC Research Center in 2008 examined the track record of companies using COSO 92 to support representations on accounting control effectiveness. Two of that study's key conclusions are reproduced below:

High Error Rate of CEO/CFO Conclusions *A high rate of senior management of Accelerated Filers reached inaccurate conclusions on the effectiveness of their company's controls despite the commitment of significant human and financial resources in implementing SOX Section 404 requirements.*

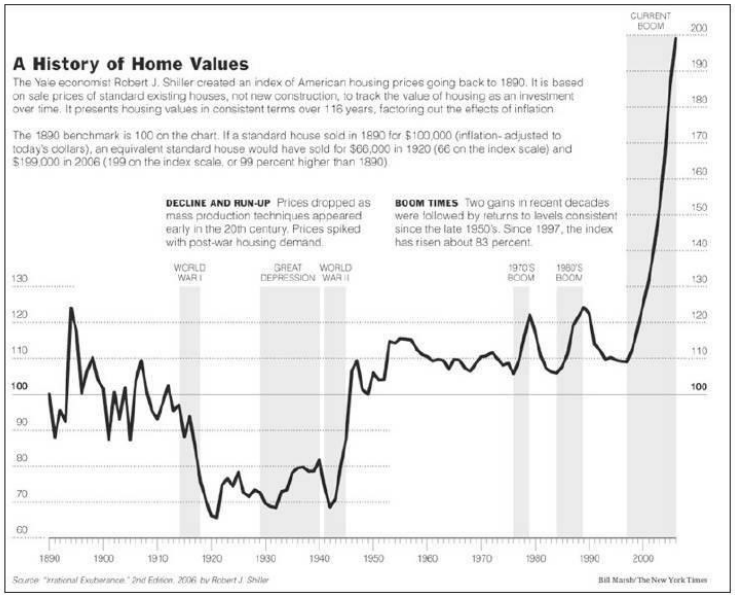
High Error Rate of External Auditor Opinions *Auditors of the same companies also concluded that accounting controls were "effective" (i.e., capable of preventing material errors in the financial*

[5] *Criteria of Control, Canadian Institute of Chartered Accountants, 1995*
[6] *Internal Control and Financial Reporting: Guidance for Directors of Listed Public Companies Registered in the U.K., December 1994.*

statements). In addition to their reports on control effectiveness, the auditors also certified that the original financial statements were fairly presented. An important underlying premise of the Sarbanes-Oxley Act is that auditors should be better equipped to provide reliable opinions on the financial statements if they have better information on the reliability of the internal control systems that support the financial statements. To date, at least on the surface, restatement trend statistics appear to contradict this assumption since the frequency of total restatements in absolute terms has increased in the post-SOX era.[7]

Coincident with the release in February 2008 of the IMA research study on the effectiveness of COSO 92 for SOX 404 reporting was the onset of the 2008 Global Financial Crisis. All, or virtually all, of the companies at the root of the 2008 global financial crisis reported having effective accounting control frameworks in accordance with COSO Internal Control – Integrated Framework in the periods leading up to the 2008 global crisis. Those financial statements included trillions of dollars of overstated assets. We believe that had those companies focused on assessing effectiveness of their risk management processes there would have been a significantly greater probability that the risk underlying assets were becoming increasingly overvalued would have been recognized much sooner. A chart developed by Robert Shiller at Yale University below graphically illustrates the growing risk of overvaluation. Our arguments for focusing on effectiveness of risk management processes are described in detail in our article "Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act at http://www.palgrave-journals.com/jdg/journal/v8/n4/full/jdg201118a.html.

BELOW Figure 1: Historic Home Values; Source: Robert J. Shiller, via The New York Times



Source: Shiller, Robert J. (2006) Irrational Exuberance. 2nd edition.

[7] Accounting Control Assessment Standards: The Missing Piece in the Restatement Puzzle, Institute of Management Accountants Finance GRC Research Practice, February 2008

PREMISE #3 - There is no urgent need for a fundamentally different approach to control assurance.

Following the 2008 global financial crisis major commissions were convened to study what went wrong. They concluded that deficient risk management and board risk oversight were two of the root causes of crisis. The vast majority of the companies at the root of the global crisis use COSO 92 as the foundation for their accounting control effectiveness representations. Shortly after the release of those studies the SEC and other security regulators including regulators in Canada, the UK, Australian and other countries required new public disclosures describing how boards of directors oversee the effectiveness of risk management processes in proxy statements and annual information forms.

Unfortunately, at the current time, as a direct result of the SEC's refusal to date to deem ISO 31000 or COSO ERM "suitable" assessment frameworks for SOX 404, companies must use one framework (COSO 92) to report on accounting control effectiveness, and another framework (ISO 31000 or COSO ERM 2004) as the foundation for their enterprise risk management ("ERM") work. This is a massively costly and unnecessary burden on public companies and their shareholders. This burden on public companies will remain if COSO 2012 is implemented in the form proposed in the December 2011 exposure draft.

OUR RECOMMENDATIONS FOR TRANSFORMATIONAL CHANGE

We believe the time has come for an "Integrated Risk and Assurance Framework". This framework would, in essence, merge work products COSO has created over the past 20 years and other best practice thinking from around the world in one integrated risk and assurance assessment and reporting framework. This new integrated framework would include all key areas of emphasis, including board oversight of risk and control, enterprise risk management, the importance of aligned reward systems, and other areas of deficiency considered to be root causes of the 2008 global financial crisis. The framework would help organizations better manage the full range of objectives necessary to be successful over the longer term and related risks that create uncertainty regarding their achievement, and support public CEO/CFO/Auditor representations on the effectiveness of those processes.

Recommendation #1 - Suspend all efforts to update COSO 92 and work with IFAC to produce international guidance.

We recommend COSO suspend all efforts to produce an incrementally improved version of COSO 92 and work with the International Federation of Accountants ("IFAC") to produce a concise, internationally accepted, truly integrated risk and assurance framework, a framework that would have true global input and an inclusive global development process. This framework would integrate the best elements from COSO 92, COSO ERM 2004, COSO 2012 ED, IFAC's December exposure draft "Evaluating and Improving Internal Control in Organizations December 2011", ISO 31000, COSO guidance on board oversight of risk, COBIT, COSO March 2012 guidance on board decision making, OCEG GRC Maturity Model, the Canadian CoCo framework, the UK Combined Code, the Walker Review in the UK, South Africa principles defined in King III, and others.

The new framework should focus on helping organizations design and evaluate the effectiveness of their processes to define and communicate objectives and assess the adequacy of the related "risk treatment" strategies and processes – both macro level and micro. The framework would be capable of supporting CEO/CFO accounting reliability representations and also support effectiveness representations on risk management processes covering the full range of important business objectives. The "principled performance" focus defined as a core vision by OCEG[8] has particular appeal as a core principle. Ideally, the older and now increasingly obsolete term, "internal control", would be replaced by the more relevant and contemporary term "risk treatment", and other terms defined in ISO 31000 risk management standard and ISO Guide 73 standard for international standard setters.

Given the global movement to adopt global accounting and auditing standards, including initial steps in the U.S., we believe that proliferating more national guidance and standards that do not reflect true

[8] *Open Compliance & Ethics Group, http://www.oceg.org/view/20055*

international input and process and result in a fragmented, inefficient and ineffective approach to risk and control effectiveness representations is not in society's best interests.

Recommendation #2 – Discontinue the current practice of using public accounting firms on a pro bono basis to drive framework research and development. Recommend that the SEC and national securities regulators around the world levy a fee on public companies to fund research, development, and continuous improvement efforts related to the new global risk and assurance effectiveness reporting framework.

COSO has been funded since its inception in the 1980s by the generous efforts of its members, and pro bono contributions of public accounting firms including Coopers & Lybrand, PwC, Grant Thornton and, most recently, KPMG. Effective corporate governance is too important to relegate to the equivalent of charity status. Investors around the world and whole national economies are negatively impacted when massive corporate failures like Enron, World Com, the financial crisis of 2008, MF Global, and other similar corporate governance failures occur. An international "Risk and Assurance Effectiveness Standards Committee" (or a similar name) should be created and funded. Methods to fund the development of all international accounting and reporting standards and guidance must be found that best protect the interests of the key stakeholder groups that rely on the information.

Tim J. Leech FCA CIA CCSA CRMA CFE is Managing Director Global Services at Risk Oversight Inc. ("RO") RO focuses on helping companies more effectively manage risk and assurance to meet escalating due diligence expectations and add real value. He has over 25 years of experience in the ERM, internal audit, and forensic accounting fields, including expert witness testimony in civil and criminal proceedings and global experience helping public and private sector organizations with internal audit transformation initiatives and the design, implementation, and maintenance of integrated GRC/ERM frameworks. He is co-author with his daughter, Lauren Leech CA CIA CFE CRMA, of "Preventing the Next Wave of Unreliable Financial Reporting: Why U.S. Congress Should Amend Section 404 of the Sarbanes-Oxley Act", and author of a new Risk Oversight Inc. white paper challenging traditional approaches to ERM titled THE HIGH COST OF ERM HERD MENTALITY. (http://riskoversight.ca/)

In 1997 Leech was awarded the designation Fellow of the Institute of Chartered Accountants (FCA) in recognition of his public service and contributions in the fields of risk and control management. In September 2009 Tim was awarded the first Outstanding Contributor to the Profession of Internal Auditing award by IIA Canada in recognition of over 25 years of global service. Leech has provided training for tens of thousands of public and private sector professional accountants, auditors and risk management specialists in Canada, the U.S., the EU, Australia, South America, Africa and the Middle and Far East. He has received worldwide recognition as a pioneer, thought leader and trainer.