COSO — Is "it" fit for purpose?
Tim J. Leech

The title of this chapter begs a question - What is "it"? Many think the term COSO refers to a now fairly dated four volume control framework originally issued in 1992 titled Internal Control – Integrated Framework. Others know COSO is the commonly used name for an unincorporated, loosely constituted private sector committee formed in the U.S. in 1985 in response to the savings and loan crisis. This chapter explores two important questions:

1. Is COSO, the committee originally formed over 20 years ago to sponsor a research study, a study commonly known as the Treadway Commission after its Chairman James C. Treadway, as currently constituted, still "fit for purpose" and, more importantly,

2. Is the 1992 Internal Control – Integrated Framework, a COSO Committee work product now approaching its 15th birthday, up to the task of meeting new, complex, onerous and hugely important expectations imposed on it by the Securities and Exchange Commission to serve as GENERALLY ACCEPTED RISK AND CONTROL ASSESSMENT PRINCIPLES ("GARCAP") for major public and private sector organizations around the world?

For those that like to "cut to the chase" the answer proposed here is an unequivocal NO to both questions.

THE ROOTS OF COSO

In the 1970s, as a result of a series of highly publicized corporate reporting failures and a loud public outcry, the American Institute of Certified Public Accountants funded The Commission on Auditor's Responsibilities, better known as the Cohen Commission. The Commission task was to:

> *develop conclusions and recommendations regarding the appropriate responsibilities of independent auditors. It should consider whether a gap may exist between what the public expects and needs and what auditors can and should reasonably expect to accomplish. If such a gap does exist, it needs to be explored to determine how the disparity can be resolved.*

A key element of the study was to determine why an alarming number of external auditor opinions on public company financial statements were subsequently being proven wrong. To reduce the incidence of auditor opinion failure the Commission concluded that:

> *A major step in implementing the Commission's proposed evolution, which should be adopted as soon as possible**, would require the auditor to expand his study and evaluation of the controls over the accounting system to form a conclusion on the functioning of the internal accounting control system**. If the auditor finds material weaknesses in the internal accounting control system, and those weaknesses are not corrected, material deficiencies may occur in the preparation of accounting information or in the control of the corporation's assets.*

This visionary 1977 recommendation was, unfortunately and for all intents and purposes, ignored. The Chairman of the landmark Cohen Commission, Manuel F. Cohen, died before the Commission's report was released.

In 1985 five not-for-profit organizations, the American Institute of Certified Public Accountants, the American Accounting Association, The Institute of Internal Auditors, the National Association of Accountants (now the Institute of Management Accountants), and the Financial Executives Institute banded together and formed the ***Committee of Sponsoring Organizations of the Treadway Commission*** to sponsor and fund another study of what had, once again, become a highly visible and widespread problem – fraudulent financial reporting. The Chairman of the Commission was James C. Treadway Jr. That Committee became best known as a result of self-proclamation as COSO. COSO's stated founding mission in 1985 was **"to identify causal factors that can lead to fraudulent financial reporting and steps to reduce its incidence**" - an ambitious and noble goal at the time that is still relevant today.

In the October 1987 the Treadway Commission's final report recommended that *"**The Commission's sponsoring organizations should cooperate in developing additional, integrated guidance on internal control**."*

Another key recommendation of the Treadway Commission built on recommendations made by the Cohen Commission a decade earlier:

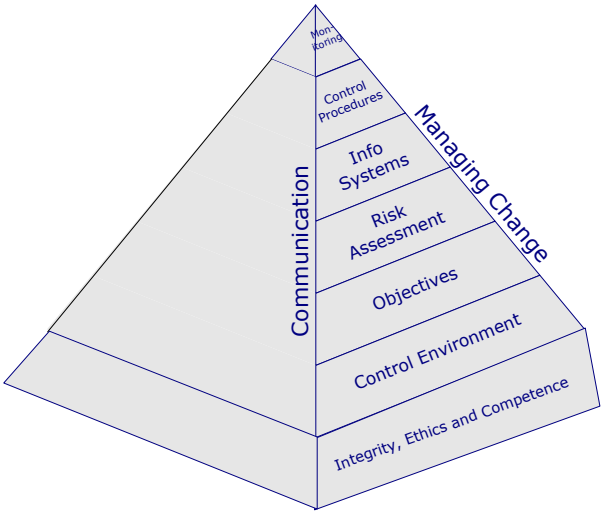
> *All public companies should be required by SEC rule to include in their annual reports to stockholders management reports signed by the chief executive officer and the chief accounting officer and/or the chief financial officer. The management report should acknowledge management's responsibilities for the financial statements and internal control, discuss how these responsibilities were fulfilled, and **provide management's assessment of the effectiveness of the company's internal controls.***

This visionary recommendation that a public company's management should formally acknowledge responsibility for, and report on, the effectiveness of internal control was, for all intents and purposes, ignored for another 15 years until the signing of the Sarbanes-Oxley Act in 2002.

As a direct result of the Treadway Commission recommendation in 1987 that the Commission's sponsoring organizations develop guidance on internal control, the

Committee of Sponsoring Organizations of the Treadway Commission, now known generally as the COSO Committee, developed and issued a ground breaking exposure draft on March 12, 1991 titled Internal Control – Integrated Framework. The primary authors of this framework were partners and staff of Coopers & Lybrand, one of the "BIG 8" auditing firms in existence at the time. (NOTE: Coopers & Lybrand has now become PricewaterhouseCoopers in the era of "the big four"). The 1991 COSO framework exposure draft illustration and definition of the term "internal control" is shown below.

COSO 1991 Exposure Draft Proposal



The Definition

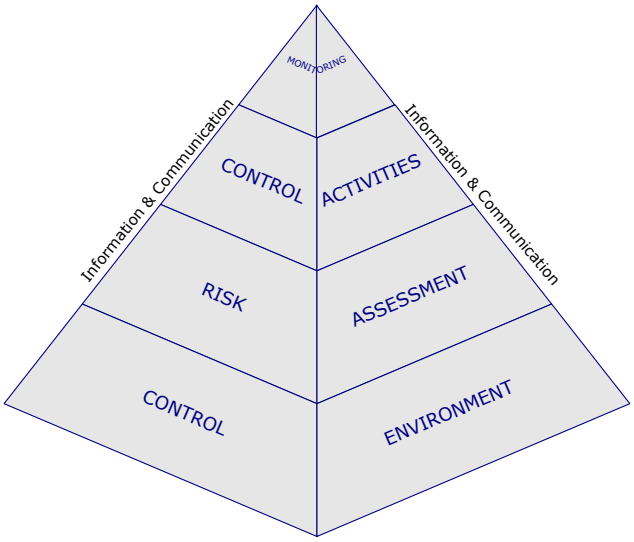
Internal Control is the process by which an entity's board of directors, management and/or other personnel obtain reasonable assurance as to achievement of specified objectives; it consists of nine interrelated components, with integrity, ethical values and competence, and the control environment, serving as the foundation for the other components, which are: establishing objectives, risk assessment, information systems, control procedures, communication, managing change, and monitoring.

As a result of an aggressive counter lobby from the "old guard" auditor faction the final version of Internal Control - Integrated Framework released in 1992 reduced the number of control categories from 9 categories to 5 and made major changes to the definition of internal control to make it more closely conform to definitions that had been in use in the U.S. by external auditors for many years prior.

> *"a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*
>
> *Effectiveness and efficiency of operations*
> *Reliability of financial reporting*
> *Compliance with applicable laws and regulations."*

This framework identified five interrelated components – Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring. A diagram depicting the COSO 1992 framework is shown below.

COSO 1992 Final



By far the most hotly debated change between the COSO 1991 exposure draft and the 1992 final framework was the treatment of "Objectives". In the 1992 version of the framework it indicates that the decision was that the establishment of entity-level objectives, including mission and value statements and strategic planning, are "management activities" but not part of an integrated control framework (page 17 of the 1992 framework volume). This was explained at the time as follows:

> *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 it is not part of internal control, was adopted.*** *The final report recognizes this distinction, and discusses objective setting as a precondition to internal control. (page 110 Internal Control-Integrated Framework, Framework volume September 1992)*

The decision to eliminate the objective category as an element of internal control in 1992 has now been, at least in part, contradicted by the COSO Committee's July 2006 Smaller Public Company guidance ("COSO SPC"). In that report it states:

> *The COSO framework recognizes that an entity must first have in place an appropriate set of financial reporting objectives. At a high level, the objective of financial reporting is to prepare reliable financial statements, which involves attaining reasonable assurance that the financial statements are free from material misstatement. Flowing from this high*

level objective, management establishes supporting objectives related to the companies business activities and circumstances and their proper reflection in the company's financial statement accounts and related disclosures. These objectives may be influenced by regulatory requirements or by other factors that management may choose to incorporate when setting its objectives. (page 10 Volume II: Guidance)

Apparently readers are asked to accept that the establishment of objectives is central to effective control but not part of an integrated internal control framework. This logic has been rejected by teams in the UK and Canada that studied the strengths and weaknesses of the 1992 framework prior to proposing their own proposals for the elements of an integrated control framework.

COSO THE COMMITTEE AND COSO THE 1992 INTEGRATED CONTROL FRAMEWORK: HAVE THEY STOOD THE TEST OF TIME?

It is important to note that the 1992 version of the COSO Internal Control - Integrated Framework has not been modified in any significant way since it was released more than 14 years ago. Unlike the Malcolm Baldrige and ISO quality frameworks that both require that the criteria be regularly revisited and improved based on user feedback, there is no similar improvement process in place for the COSO 1992 framework. Some of the COSO Committee member organizations have claimed that this is because the 1992 framework has "stood the test of time". The Institute of Management Accountants, a founding member of COSO, has voiced concerns on this point but to date has been unable to get the support of the other COSO Committee members to undertake an update of the framework.

The fact that there is no improvement process in place for the 1992 COSO Internal Control - Integrated Framework is likely explained by the fact that COSO is, in reality, not an organization in the usual sense but rather a loosely constituted committee that meets a few times a year. As a Committee it has no legal existence, no corporate governance structure, no funding mechanisms, no physical address, and is not overseen by any regulatory body. There is also currently no mechanism in place to fund the COSO Committee's projects beyond contributions from sponsoring organizations. To illustrate their financial limitations the COSO Committee has recently released a request for proposal for a consulting firm to help with its latest project on monitoring of internal control. Firms interested in bidding are cautioned in the COSO RFP issued on October 17, 2006 that:

COSO is a volunteer committee with limited resources. Typically the COSO Board has reimbursed developers for out-of-pocket expenses only (e.g., reasonable travel and administrative costs) The business benefit to the developer is that the developer is identified directly with the COSO end-product as part of the globally recognized COSO brand.

What this caution really means is that those that apply to act as primary COSO researchers and authors should be prepared to accept public relations benefits in lieu of being paid. This 'pro bono"/donation approach to research and standard writing has been how the majority of work undertaken by the COSO Committee to date has been done, including the guidance issued by the COSO Committee on enterprise risk management in 2004 and guidance for smaller public companies issued in 2006. Both of these more current work products are heavily linked to the original, unchanged 1992 five category framework. Both of these work products were authored by PricewaterhouseCoopers in return for the right to be formally linked to the COSO brand.

It is important to note that since the COSO Internal Control – Integrated Framework was released in 1992, the Committee has made no attempt to rigorously monitor acceptance and use of the framework or periodically assess in a formal way whether the framework could, and should, be improved. The rigorous analysis of the strengths and weaknesses of the COSO 1992 framework that has been done in other countries in the mid 1990s, including Canada and the U.K., have not been formally acknowledged by the COSO Committee.

ACTUAL MARKET ACCEPTANCE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX

Voluntary market acceptance of the value of the COSO 1992 framework as a tool for management and auditors prior to the enactment of Sarbanes-Oxley can be seen from the statistics below. These findings are part of a rigorous research study on the use of the COSO 1992 framework conducted by Professor Parveen Gupta under the sponsorship of the Institute of Management Accountants.

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)

The largest number of respondents indicated that the 1992 COSO framework was not used to any extent in their company prior to the enactment of the Sarbanes-Oxley Act in 2002. Only a very small number of companies indicate that they used the COSO 1992 framework to a large extent.

During the period of 1992 to 2002 the Institute of Internal Auditors and American Institute of Public Accountants, two of the five founding members of the COSO Committee, made some attempts to promote and educate its members on the value and benefits of using the COSO control framework through training workshops, publications and integration with certification curriculum although limited knowledge of COSO 1992 was required for certification in these organizations. The other three COSO founding members did relatively little during this period to aggressively promote why, or how, the COSO 1992 Internal Control- Integrated Framework could or should be used by their members. The business case for using the COSO framework has not been well articulated, communicated or accepted by the majority of the business community.

EXPECTATIONS OF COSO ESCALATE OVERNIGHT

When the SEC released final guidance for Section 404 in 2003, as a general statement, they mandated the use of the COSO control framework for assessing internal control over financial reporting by every public company listed on a U.S. exchange by stating that the COSO 1992 Internal Control – Integrated Framework met their "suitability" criteria for SOX control assessments. The SEC said that to qualify as a suitable assessment framework the framework must:

1. Be free from bias.
2. Permit reasonably consistent qualitative and quantitative measurements of a company's internal control.
3. Be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted.
4. Be relevant to an evaluation of internal control over financial reporting.

Although the SEC said in footnote 67 of Section 404 Final rule that "The Guidance on Assessing Control issued by the Canadian Institute of Chartered Accountants and the Turnbull Report published by the Institute of Chartered Accountants in England & Wales are examples of other suitable frameworks", they were unequivocal when they stated:

The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements.

Concluding that the 1992 COSO Internal Control – Integrated Framework was capable of fully meeting all four criteria was a massive untested assumption on the part of the SEC that has now been identified as a major contributing factor to the massive confusion and

costs that have occurred as U.S. listed public companies attempted to comply with sections 302 and 404 of SOX.

IS COSO 1992 FREE FROM BIAS?

In real life the goal of producing work products that are totally free of any bias is an elusive one. When we are asked as individuals to undertake any task in life it is very difficult if not impossible not to bring our collective experiences and biases to the table. All COSO work products to date have been authored by professionals that have an "AUDIT BIAS". Although the COSO Committee members include organizations that represent management accountants, financial executives, internal auditors, accounting academia and external auditors, the perspectives and historical viewpoints of the internal and external audit professions have dominated to date. Many internal auditors have external audit backgrounds. An external auditor background generally results in viewpoints that are quite different from those held by others engaged in assurance activities like quality professionals, risk professionals, IT specialists or even generic management consultants. The biases are influenced by the training and accreditation process for their respective disciplines.

The term internal control is itself an internal/external auditor invention that doesn't exist in any real way in the realm of quality or risk management, and is rarely used by business unit staff in their daily work. Quality professionals use frameworks like Malcolm Baldrige, Six Sigma, ISO 9000 and ISO 17799 as their "frameworks" to ensure desired outcomes are achieved. They talk about ensuring process reliability. Risk professionals use philosophies found in frameworks like the Australia/New Zealand Risk Management standard 4360. They talk about achieving the goal of assessing and analyzing risk and seeking agreement on acceptable levels of residual risk. IT professionals use frameworks like COBIT and ITIL. Their goal is usually to examine a client's environment for conformance to those frameworks. Management consultants use methodologies like "Balanced scorecards" and talk in terms of strategic priorities, key result areas, and key performance indicators.

ANSWER: From a purist perspective, COSO Committee work products produced to date have not been "free from bias".

DOES COSO 1992 PERMIT CONSISTENT QUANTATIVE/QUALITATIVE MEASUREMENT?

Evaluation frameworks such as Malcolm Baldrige put enormous emphasis on the importance of measurement controls in the pursuit of quality. Baldrige, unlike the COSO Internal Control – Integrated Framework, is a numerically weighted framework that allows a score to be generated on a company's quality system out of total possible 1000 points. None of the COSO frameworks have numeric weightings or any type of guide for management or auditors to assign numeric scores. Very little guidance is provided for

users on how to evaluate qualitative information and reach "effective/ineffective" conclusions on internal control although the 2006 COSO guidance for smaller public companies did make advances in this area. To meet this suitability test a framework would have to be capable of generating reasonably consistent conclusions from multiple teams when given the same set of facts. None of the three primary COSO guidance documents produced to date (COSO Internal Control-Integrated Framework, COSO ERM or COSO Smaller Public Company) were ever intended or designed to accomplish this goal.

ANSWER: From just about any perspective, the COSO Committee work products produced to date do not permit reasonably consistent quantitative/qualitative measurements of internal control.

IS COSO 1992 SUFFICIENTLY COMPLETE SO THAT RELEVANT FACTORS ARE NOT OMITTED?

The original mission of the Treadway Commission was **"to identify causal factors that can lead to fraudulent financial reporting and steps to reduce its incidence**". A key recommendation was to develop an internal control framework that would support this aim. The current SOX requirements issued by the PCAOB call for a specific analysis of the control capabilities to prevent and detect fraud. An IMA research study completed in September 2006 on the use of COSO 1992 for SOX indicated that very few companies used the COSO 1992 framework as the primary assessment guidance to do this task. On average less than 1 in 4 respondents indicated that they used COSO 1992 to a large extent to complete this dimension of their assessments. Other surveys conducted indicate that most companies used guidance issued by the Association of Certified Fraud Examiners or the AICPA to examine the existence and quality of controls. The IMA study also indicated that more than 25% of respondents indicated that they did not complete any formal antifraud assessment.

On other fronts, most people acknowledge that in today's world, IT plays a huge role in the processes used to generate external financial disclosures and that weak IT controls can result in material errors in financial statements. The same IMA research study indicated that more than 60% of respondents did not use COSO 1992 to assess the adequacy of IT controls. Almost 52% of respondents indicated they used the CobiT framework issued by the IT Governance Institute.

Answer: Unless one accepts that fraud prevention and detection and IT are not relevant factors when opining on the adequacy of internal control over financial reporting the COSO framework does not meet this criteria.

IS COSO 1992 RELEVANT TO AN ANALYSIS OF CONTROLS OVER FINANCIAL REPORTING?

The events that resulted in the enactment of SOX all had a common theme – a significant breakdown of oversight and ethics at senior levels of public companies including the

audit committees of these corporations. Most people with knowledge of the facts that led to SOX agree that the number one risk to reliable financial reporting is a lack of ethics on the part of senior level employees. Although there are no hard statistics available, there is evidence that supports the view that the number two biggest risk to reliable financial disclosures is inadequate knowledge/capability on the part of senior financial accounting staff. The unverified number 3 biggest risk, although one could advance an argument that it is the number one risk, is the competence and integrity of the external auditors hired to audit and report on the financial statements produced by management.

While it is indisputable that COSO 1992 does include some discussion of the need for "tone at the top" it provides little in the way of specifics on how to measure whether controls to ensure sound ethics are "effective". If one wants to see a framework that emphasizes how to evaluate the adequacy of controls important to compliance and ethics the best and newest guidance available is from a new organization called Open Compliance and Ethics Group. (www.oceg.org) COSO 1992 certainly does not provide much, if any, specific guidance on how to evaluate the controls to ensure that financial accounting personnel possess sufficient competence or the controls at CPA firms to ensure high ethical conduct on the part of partners and staff. Again, the newer COSO SPC framework has made some advances in this area.

Answer: COSO is relevant but not optimal for evaluating the adequacy of controls to address the three biggest risks to reliable financial reporting.

COSO: LOOKING FORWARD

Concerns regarding the adequacy of the COSO Internal Control – Integrated Framework have been reported by a wide range of respondents to the SEC and PCAOB. The SEC has not directly addressed the question of the challenges that have been raised regarding the "suitability" of COSO 1992, or the brand new COSO for Smaller Public Companies guidance, but indirectly has signaled an answer. The SEC has announced plans to develop and issue its own guidance how to assess and report on Internal Control. This guidance is expected to be issued in exposure draft form in December 2006. The IMA has publicly stated that they believe that the COSO 1992 was never intended to meet the criteria defined by the SEC and that it does not fully meet all of the defined suitability criteria for SOX. To date none of the other COSO Committee organizations have publicly stated their position as to whether the 1992 COSO Internal Control – Integrated Framework fully meets all four of the suitability criteria defined by the SEC.

In a letter to the SEC dated September 18, 2006, in response to an SEC request for comments on a Concept Release related to SOX (www.sec.gov/comments/s7-11-06/s71106-98.pdf) Larry Rittenberg, the current Chair of the COSO Committee, closed with the following hints on the way forward:

COSO is embarking on a strategic planning process to adapt to the changing environment. The COSO Board has recognized that a new infrastructure may be needed for COSO to address internal control and risk management issues on a more timely fashion. The Board has discussed projects such as using the internet to enhance the sharing of control information, a project on assessment, and a project identifying effective monitoring of controls. The Board also seeks to address many longer-term issues, such as harmonizing control frameworks and becoming more inclusive as an organization. The Board is committed to improving the practice of internal control implementation as well as internal control reporting on a more cost-effective manner for all firms. We welcome the opportunity to work with the SEC in accomplishing our mutual objectives in this area. We seek the SEC's input on these important endeavors.

Time will tell whether COSO the framework or COSO the Committee are "FIT FOR PURPOSE". Stay tuned.

AUTHOR NOTE: This article was published as Chapter 3 of THE GOVERNANCE RISK AND COMPLIANCE HANDBOOK, Anthony Tarantino editor, published by Wiley in 2008.