

From “Leech talks risk”

Tim Leech, CIA, FCA, CFE, founder and Managing Director of Leech & Co GRC Inc., is recognized globally as a thought leader and one of the pioneers of the control and risk self-assessment (CRSA), enterprise risk management (ERM), and governance, risk, and compliance (GRC) movements

The Best 112 Swiss Francs You Will Ever Spend

The best single source of guidance for internal auditing issued to date, in my estimation, was released in final form this month by the International Organization for Standardization (ISO). The full title is *Risk Management—Principles and Guidelines* (ISO 31000). A single-user license can be purchased from the ISO's [Web site](#) for 112 Swiss francs (about US \$111 based on today's exchange rate).

This guidance represents more than 20 years of development drawing on experience and insights of organizations around the world. The roots of this document are the Australian/New Zealand Risk Management Standard 4360 originally released in the mid-1980s. Hats-off to the Aussies and Kiwis for kicking-off the start of what I hope will be a transformation in global thinking, particularly in the internal audit community. It's too bad more U.S. financial institutions at the root of the current global economic crisis and their regulators didn't embrace the core tenets in this document. Billions of people around the world would be better off today. The worry is that these “too big to fail” financial institutions may still not be following the principles in this document. U.S. regulators should seriously think about mandating the use of this guide as principles-based guidance as well as mandating the use of it across all levels of government.

The definitions in ISO 31000, while representing some compromise, are the best and most concise I have seen. For example, in paragraph 2.26 *control* is defined simply as “measure modifying risk.” Note 2 to the definition quite correctly states, “Controls may not always exert the intended or assumed modifying effect,” — a truism, albeit a massive understatement in many organizations.

The length of the document is as short as I think is possible while still conveying the key information. This document could be used by an internal audit department that is still “control/compliance centric” to transform existing audit approaches to true risk-based assessments.

Annex A—Attributes of Enhanced Risk Management could be used by an internal audit department to form the core audit criteria to complete an audit of the effectiveness of risk management processes required by IIA Professional Practice Standard 2120.

I believe that all internal auditors should use the approach to assessment described in this new global standard on all traditional direct-report audit engagements and when facilitating work-unit risk assessments. Internal auditors also should work

relentlessly to help their organizations implement the attributes of enhanced risk management described in Annex A. The Introduction to 31000 concisely describes the benefits that flow from using effective risk management processes.

I don't often give glowing reviews on anything, but I think this one is a winner. The IIA would do well to retool all its training courses and convene a full conference on how to best implement ISO 31000.

This is a short document that has the potential to change the face of internal auditing as we know it — if the profession is willing to change. Are you?

Share This Article:



Posted on Nov 19, 2009 by [Tim Leech](#)

[Comments \(1\)](#) un-categorized

1. Comment by: **Dan Clayton** (11/20/09 08:03 AM) <http://www.chanllc.com>

What fascinates me about ISO 31000 is section 2, Terms and Definitions. To me these simple definitions will help the conversation start on the same footing. As I have attended Audit Committee meetings, I am always interested to see how each person defines risk. It generally is defined by the individual's background. If they were compliance, risk is regulatory; if they were accountants, risk is financial impact. What ISO 31000 does is say that risk is broader and must be placed in context of how it impacts business objectives. It then goes further defining the external and internal context for risk. I believe they could have gone even farther and linked risk management to good management, but at a minimum, ISO 31000 is a great step in unifying the language between management and assurance providers

ISO 31000 - Is It a "Suitable" Framework for Sarbanes-Oxley Section 404 Reporting?

When the U.S. Securities and Exchange Commission (SEC) issued interpretative guidance on management reporting pursuant to section 404(a) of the U.S. Sarbanes-Oxley Act in 2002 they stated that the 1992 Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control-Integrated Framework* met their criteria for a "suitable" framework. The SEC left the door open for new and better control reporting frameworks when they stated, "*other evaluation standards exist outside of the United States, and that frameworks other than COSO may be developed within the United States in the future, that satisfy the intent of statute without diminishing the benefits to investors*" (page 9 of 13 of Release 33-8238).

Since 2003, thousands of CEOs, chief financial officers, and external audit partners have formed opinions on control effectiveness using the 1992 COSO *Internal Control-Integrated Framework* that have subsequently proven via restatements to be materially wrong using SEC materiality criteria. Although it is unclear, given the high error rate in these control effectiveness representations, whether investors, regulators, and other key stakeholders place much reliance on these representations, what is clear is that they have cost investors billions of dollars in the form of incremental internal costs and fees to public accounting firms.

In November 2009 the International Organization for Standardization (ISO) issued a new risk management standard, ISO 31000. It is the product of years of development and input from a wide range of highly respected risk and control professionals around the world. It is almost certain to become the internationally accepted risk management standard. ISO requires all standards they issue to be reviewed and improved every four years — an approach COSO has clearly rejected since the COSO internal control framework has not been revisited with the intent of improving it since it was issued in 1992. At this point in time COSO has no plans that I am aware of to ever review or improve the core COSO internal control framework, or to study why thousands of senior executives and external auditors have arrived at materially wrong conclusions using it. Apparently, the COSO members consider the 1992 internal control framework to be something akin to the Bible — guidance intended to last centuries without revision or need for improvement.

The term *effective control* is another way of saying *tolerable residual risk*. Based on research I have done over the past eight years I believe that ISO 31000 better meets the "suitability" criteria for Sarbanes-Oxley Section 404 reporting defined by the SEC in 2003, and that the SEC should formally endorse it as a framework that meets its Sarbanes-Oxley Section 404 control effectiveness reporting suitability criteria.

Recognizing the harsh reality that what Tim J. Leech thinks is not of any

real significance when it comes to Sarbanes-Oxley reporting rules — and in many other areas where I sometimes foolhardily venture opinions — I decided to take the bull by the horns, as the old expression goes, and just ask the SEC for an opinion.

What follows below is the text of the electronic request I made to the Office of the Chief Accountant at the SEC today via a page on its Web site titled "Corporation Finance Request Form for Interpretive Advice and Other Assistance." I will keep you posted on whether the SEC thinks the question I have posed is significant enough to warrant a response. The SEC has electronically promised a response within one business day.

INQUIRY TO THE SEC FILED BY TIM LEECH FEBRUARY 2, 2010

Release 33-8238 Management's Report on Internal Control Over Financial Reporting states that "the final rules do not mandate use of a particular framework, such as the COSO Framework, in recognition of the fact that other evaluation standards exist outside of the United States, and that frameworks other than COSO may be developed within the United States in the future, that satisfy the intent of the statute without diminishing the benefits to investors." (Page 13 of 93)

The guidance goes on to state, "Specifically, a suitable framework must: be free from bias; permit reasonably consistent qualitative and quantitative measurements of a company's internal control; 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; and be relevant to an evaluation of internal control over financial reporting." (Page 14 of 93)

In late 2009 ISO released a new International Standard, ISO 31000, titled Risk Management – Principles and Guidelines.

It is my belief that ISO 31000 meets the four suitability criteria defined by the SEC in the Final Rule and is capable of producing more reliable representations on the effectiveness of internal control over financial reporting.

Can you please advise me whether the SEC considers ISO 31000 to be a suitable framework for reporting on internal control effectiveness pursuant to Section 404 of the Sarbanes-Oxley Act and related SEC regulations?

Relevant research related to this request includes the following:

1. Internal Control: COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices, Parveen P. Gupta, LLB, Ph.D., Institute of Management Accountants, 2006.
2. *Governance, Risk, and Compliance Handbook*, Anthony Tarantino, Wiley, Chapter 3, COSO – Is It Fit For Purpose?, Tim J. Leech, page 65.
3. ISO 31000, Risk Management – Principles and Guidelines, First Edition, 2009-11-15.

4. The Global Meltdown & COSO 1992, Leech Talks Risk, *Internal Auditor Online*, December 4, 2009, (<http://bit.ly/bwV1PZ>).
5. Accounting Control Assessment Standards: The Missing Piece in the Restatement Puzzle, Discussion Paper, Institute of Management Accountants, February 2008.

Stay tuned for the SEC's response to my request.

Share This Article:



Posted on Feb 2, 2010 by [Tim Leech](#)

[Comments \(4\)](#) un-categorized

1. Comment by: **Arnold Schanfield** (2/7/10 12:53 PM)

Hi Tim:

A very smart blog!! ISO 31000 was developed by a group of smart individuals and is being accepted as the go to risk management framework. The COSO framework while it had some good ideas in it, is tired looking and has not been updated since 1992 as you have clearly pointed out. It has been rejected reasons I articulated in my response to Richard Chambers blog of this past November. it needs to be scrapped in its entirety or reworked with adequate representation from the risk management communication

PCAOB Release 2003-017 said that while the COSO 1992 framework provide a suitable framework for "internal control", "other suitable frameworks have been published in other countries and likely will be in the future." This thinking became part of the SEC's final rule on management reports. (<http://www.sec.gov/rules/final/33-8238.htm>); The SEC (or PCAOB) subsequently published advice that other internal control codes could be used. Most of the Big 4 still blatantly misinterpret the SEC's advice to say that the COSO ERM framework is the preferred approach.

Had other frameworks been used such as precursor to ISO 31000; the framework from Australia/New Zealand AS/NZS 4360 or CoCo from Canada, it would have been immediately apparent that Sarbanes Oxely was being rolled out as bottoms up versus the top down holistic approach of ERM. This would have save companies billions of dollars. In summary, not only is ISO 31000 a suitable framework for SOX compliance but it is a best in class framework for all of risk management.

Regards,

Arnold Schanfield

1. Comment by: **Tim Leech** (2/7/10 02:15 PM) <http://www.leechgrc.com>

Arnold;

Thanks for your comment. Based on the companies I have worked with, and the years of research I did for the IMA in the US on SOX regulations the dominant framework in use for SOX is the 1992 COSO Internal Control Integrated Framework, not the 2004 COSO ERM framework. At least in COSO ERM objective setting was recognized as a key element of effective control.

I agree with you that a true "risk-based" assessment framework would have started with the big picture risks including the most statistically likely errors for the business sector the company operates in, as well as the major risks generally that have proven to produce materially wrong F/S. Unfortunately because of the legacy of AS 2 many companies do not start their assessments with or focus enough attention on the big picture risks.

Also unfortunately for investors, it is my view from observing COSO over the past 20 years, that the dominant COSO member is the AICPA. The major public accounting firms appear to be are comfortable with the old COSO 92 framework and have made a significant investment creating their COSO checklists for junior staff. Few focus their attention on measuring the residual risk of a major line item or note disclosure error.

I will be doing a blog post this week outlining the primary reasons I think ISO 31000 would produce more reliable and better overall results for SOX 404 reporting.

1. Comment by: **Arnold Schanfield** (2/8/10 06:54 AM)

Tim:

What is your e mail address?

Arnold

1. Comment by: **Douglas Hileman** (2/10/10 01:12 PM) <http://dougflashileman.com>

I am a specialist in Environmental & Sustainability auditing (30 yrs); I was in-house at a Big 4 public accounting firm when Sarbox was passed, and 6 more years. I supported financial audit teams, many internal audits focusing on various E&S risks, and have developed & audited E&S programs, systems, and controls. So - an unusual mix of experience in auditing.

I think ISO 31000 will catch on, in large part because it provides details that are more accessible to a broader range of readers. There is a risk, however, that users will implement them in a cookbook fashion, with insufficient focus on company culture, risk tolerance, management, and performance.

Many years ago, ISO 14001 (Environmental Management Systems or EMS) was hailed as the silver bullet to prevent compliance failures and to drive performance. ISO 14001 provides a very useful framework, so the practitioner can make sure s/he hasn't left anything out. The aspects & impacts analysis can be very challenging and useful - or it can just as easily be a cursory exercise, robbing the EMS development process of much of its value. As long as a company's env. mgmt program's actions and documentation match, it can be certified. The certified EMS need not be particularly good.

In my discussions w clients, I'm suggesting risk inventory & analysis using BOTH. I like the COSO categories, esp with some adaptations [financial reporting and non-financial (e.g., Sustainability) reporting, for example]. Then use ISO 31000 to build out the risk mgmt system