

December 29, 2011
Charlotte NC

Re: COSO *Internal Control – Integrated Framework* Draft for Public Exposure

I strongly support the effort to update the COSO *Framework* and by this commentary I wish to contribute to the wider acceptance and use of the disciplines of internal control and enterprise risk management. Kindly accept my observations in the spirit of forthright remarks intended to elevate the cause of risk governance reform.

In short, the updated *Framework* appears thorough and comprehensive, while perhaps more in a manner geared toward risk management professionals than as a practical guide to the design and use of highly desirable reforms. That is undoubtedly intentional, but senior managements and boards of directors may find it arduous to follow its important directives, and they're the ones who need the most convincing. Exactly how it serves to improve the likelihood of achieving objectives is less clear than the appropriately methodical process it advocates.

When I became chief audit executive of First Union in 1995 I immediately began to introduce the concepts of the original *Internal Control Framework* within my department. In 2004 (now at the merged Wachovia) following the publication of *Enterprise Risk Management – Integrated Framework*, I introduced *ERM* to the audit committee and senior management. Unfortunately, without their buy-in, the chief auditor alone has little chance of orchestrating such a sweeping change in risk governance. Beginning in 2006, along with colleagues in risk and finance, and with the assistance of PwC, we attempted to introduce an even broader and more integrated approach to managing risk. This last effort was ultimately undone by the company's demise and sale. In fact the failure of the company serves as one of the best lessons from which to learn the importance of what the *Framework* has to offer. That none of the efforts over the years succeeded in reforming the company's approach was not unique to us. A 2009 report from the North Carolina State University ERM Initiative is instructive on this point.

Why has more lasting change not taken place? I believe there are two reasons:

1. Implementation takes resources and risk governance does not directly produce revenue; a compelling case that illustrates a sufficiently rewarding return on the investment to senior management and the board is difficult to articulate.
2. Internal control and enterprise risk management are processes, and without a corresponding culture to match – one of widespread employee connection to purpose and values – process alone is unsustainable.

Both frameworks “acknowledge that risks occur at every level of the entity and result from a variety of internal and external factors. And both frameworks consider risk identification in the context of the potential impact on the achievement of objectives.”

But why two sets of standards with so much overlap? *ERM* was touted as a more complete approach, and it is. *Internal Control* specifies achievement of objectives in three categories, operations, reporting, and compliance. *ERM* added a fourth, strategic objectives. Why update the lesser version, particularly following a financial meltdown during which strategic objectives were so plainly unmet?

If, as is stated, “The original framework has gained broad acceptance and is now widely used around the world” how did so many risk management failures occur, leading to the economic crisis? By any measure, reasonable assurance was not provided. Objectives were not achieved – strategic or otherwise. For this update to be relevant, in the face of real world events so at odds with its original intent, it should explain what went wrong and how the changes will lead to better results.

With three categories of objectives, five integrated components, seventeen principles relating to the components, and eighty-one attributes relating to the principles, this *Framework* doesn't feel clarified over the original, and it does feel prescriptive, particularly given the following:

"Although each attribute generally is expected to be present within an entity, it may be possible to have a principle present and functioning without every attribute being present...However, in the absence of an attribute being present and functioning, a deficiency may still exist." Thus it is recommended to go through all the attributes to determine whether they are present and functioning, or if absent, whether that absence constitutes a deficiency. Not that this is an inappropriate exercise – the principles and attributes are instructive – but the lengthy list of prescripts comes across more like a set of rules than a principles-based approach.

From the descriptions of the use of the *Framework*, it is hard to imagine how to report on the relative strengths and weaknesses of a series of principles and attributes and avoid a checklist. Board reporting should be an integral part of every process, and giving the board perspective – not simply data – is a crucial skill. The *Framework* would benefit from additional guidance on reporting its findings in a way the board would find useful in exercising its oversight duties.

As for roles and responsibilities: "Everyone in an organization has some responsibility for internal control." True enough, but how do you get everyone to understand what that means to their daily activities? This is why a culture of employee engagement is as important as the process of internal control.

Guidelines that follow relate more explicitly that the board is expected to discuss with senior management the state of the organization's internal control system, and that senior management is to assess the internal control system using the *Framework*. This is indeed at the core of oversight. But if the board is to guide and direct management in the development and performance of internal control, as the document states, the means to that end presume an understanding on behalf of the board that is beyond most of the directors' available time and experience (the goal should be to access their collective wisdom – not to train them in skills expected of management), unless by "guide and direct" you mean "point and command." Again, the board needs perspective for exercising oversight, not details for coordinating process. And to persuade senior management, as a precondition for a discussion with the board, to embark on an assessment of internal control using the *Framework* – a challenging process to put into practice – a case must be made that is more compelling than the reasonable assurance of achieving objectives (a quality they routinely project without the *Framework* and one most board members expect is already in place).

The financial crisis pointed out serious deficiencies in risk governance. COSO has the opportunity and the resources to contribute toward a much-needed response. If the goal of this *Framework* is "to enable organizations to effectively and efficiently develop and maintain systems of internal control" it should be made more accessible to the broad audience it seeks to influence.

Attached is an article with additional thoughts and suggestions that I believe would improve the prospect for successful risk governance reform.

Respectfully,
Peter Schild
pschild@carolina.rr.com
704 849 0767