Matthew Leitch Associates Limited

www.internalcontrolsdesign.co.uk
tel +44 1372 815 856
29 Ridgeway, Epsom
Surrey, KT19 8LD
United Kingdom

Committee of Sponsoring Organizations
of the Treadway Commission

29 March 2012

Dear Committee members

Consultation on the revised framework for internal control

Thank you for the opportunity to comment on the new exposure draft. After some introductory comments, this response focuses on one crucial issue. I hope you find my analysis helpful.

I have been working on the risk management committee of the British Standards Institute for some years, helping to draft both editions of BS 31100 on risk management, and commenting on ISO's risk management standard, ISO 31000:2009. I have spent a lot of time looking at these issues. (However, the analysis and suggestions in the comments below are entirely my own.)

I personally welcome an update of the internal control framework, which provides an opportunity to solve some problems that have emerged in the years since the framework was first published. In particular:

- The related Evaluation Tools volume has inspired inefficiently designed working papers in many companies.
- Many people are confused over the difference or otherwise between internal control and risk management.
- Many are also confused by the boundaries of some of the five components of internal control and there is related confusion over what constitutes internal control and what is just the rest of management.
- Many imagine that the framework defines effective internal control, when in fact it just explains what factors to consider without actually specifying a minimum level.

The crucial issue raised by risk management

However, the exposure draft imports a lot of material on risk management, and this raises a worrying new issue.

The underlying model of risk management used is one where 'risks' are thought of as identifiable entities that can be listed and then understood, owned, and managed, largely one-by-one.

In the fields of audit and accounting, where this view of risk is common, it can seem like an entirely generic view, but in the wider world of risk management the risk-listing approach is just one option and frequently not the favoured approach in fields where there is a lot at stake.

For example, in making predictions and decisions about climate change, nuclear safety, health, pollution, and many aspects of banking and insurance the usual approach is firmly based on science and mathematics. It requires coherent, probabilistic models, often quantified, that relate factors together. Just listing 'risks' without creating a coherent model with a rationale is not considered adequate and the errors it produces are well understood and documented.

Also, risk analysis and management in high-stakes fields are usually achieved through ensuring that decision-making and other core management processes take risk/uncertainty into account, rather than through operating a separate process to manage 'risks'.

An incomplete but illustrative list of authoritative guides from various fields of application and countries, including the USA, appears here:

http://www.workinginuncertainty.co.uk/authoritative.shtml

The worrying issue raised by the exposure draft is that the framework may encourage organizations to take an approach that is illegal in some fields in some countries (including the USA), either through not meeting the more demanding requirements of regulations or statutes, or through exercising a standard of care that is far too low.

To understand exactly how serious this issue is now, and could become in the near future, would require a thorough review of guidance in many fields, applying suitable legal knowledge as well as a deep understanding of the risk management ideas involved, and the trends towards more scientific methods in each field.

Solving the issue of risk management

However, a much simpler solution to this issue seems to be to restrict the scope of the internal control framework to book-keeping, accounting, and related audit. In these fields the COSO framework more or less defines the usual standard of care and its technical recommendations are appropriate. For example:

- Treating different potential book-keeping and accounting mistakes and frauds as separate from each other is not entirely unreasonable.

- The approach to ‘risk tolerance’ that uses bands makes some sense when applied to the accuracy of financial numbers, especially if no attempt is made to relate this to specific decisions made using the numbers.

This simple restriction of scope could be done with relatively light editing of the text. It would greatly simplify subsequent debates about the content of the framework because there would be no need to write guidance applicable to all fields where risk management is applied, or respond to criticisms of the draft that are mainly motivated by concerns about other fields.

The positive contribution of the framework would not be greatly reduced by this because its main fields of application, for most organizations, have been book-keeping, accounting, and related audit, and this is unlikely to change.

A further advantage is that PricewaterhouseCoopers would no longer be expected to produce guidance to be applied to fields outside its main expertise. PricewaterhouseCoopers is a highly respected firm with great expertise in its specialist fields, but does not usually give advice on nuclear safety, pollution, health, climate predictions, or medicine, and nor should it be expected to, even indirectly.

Yours sincerely

Matthew Leitch