9499 MacArthur Blvd
Bethesda, MD 20817
Phone: +1(301) 529-8118
www.LHubbard.com

To COSO and PwC:

I am pleased to comment on the COSO Internal Control Integrated Framework draft for public exposure issued in December, 2011. I believe the draft accomplishes its purpose of increasing its relevance in the increasingly complex and global business environment so that organizations worldwide can better design, implement, and assess internal control.

I have three major comments on the draft, which are detailed in the attached document.

Comment 1: The distinction between Risk Response (part of internal control), the management actions to address the risk (not part of internal control), and Control Activities (part of internal control) is not always clear.

Comment 2: The use of a residual risk approach, whereby existing controls are identified then any additional risks are identified, should be highlighted as an effective Risk Assessment technique.

Comment 3 – Overly stress the requirement for all seventeen Principles of control to be applied.

I will be pleased to answer any questions you may have.

Larry D. Hubbard CIA, CISA, CCSA, CPA
Larry@LHubbard.com
March 30, 2012

Comment 1: The distinction between Risk Response (part of internal control), the management actions to address the risk (not part of internal control), and Control Activities (part of internal control) is not always clear.

Para 250 makes the distinction, but could be improved by clarifying the "related plans, programs, or other actions…" are management actions, not internal controls.

250 There is a distinction between risk assessment, which is part of internal control, and the choice of specific risk responses and the related plans, programs, or other actions deemed necessary by management to address the risks. Internal control does not encompass ensuring that the optimal risk response is chosen. For instance, the man-

Para 251 needs additional words for clarification, as once "management has chosen to reduce or share a risk", then management actions to respond to the risk are implemented, and "control activities can then be selected and developed."

251 Once management has chosen to reduce or share a risk, control activities can then be selected and developed. This is the focus of the following chapter. In some instances, management may select a response that requires action within another component of internal control—for instance enhancing a part of the control environment. Typically, control activities are not needed when an entity chooses to either accept or avoid a specific risk. For instance, a mining company with significant commodity price risk may

As background:

Para 246 defines Risk Response correctly, same as in COSO's ERM framework:

246 Risk responses fall within the following categories:

- *Acceptance*—No action is taken to affect risk likelihood or impact.
- *Avoidance*—Exiting the activities giving rise to risk; may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
- *Reduction*—Action is taken to reduce risk likelihood or impact, or both; typically involves any of myriad everyday business decisions.
- *Sharing*—Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk; common techniques include purchasing insurance products, forming joint ventures, engaging in hedging transactions, or outsourcing an activity.

Page 51 of the prior internal control framework also makes the distinction:

Integration with Risk Assessment

Along with assessing risks, management should identify and put into effect actions needed to address the risks. The actions identified as addressing a risk also serve to focus attention on control activities to be put in place to help ensure that the actions are carried out properly and in a timely manner.

For example, a company set as an objective "Meeting or exceeding sales targets". Risks identified include having insufficient knowledge of current and potential customers' needs. Management's actions to address the risks included establishing buying histories of existing customers

51

The COSO ERM framework, page 43, also makes this relationship clear:

Note that there is a distinction between risk assessment, which is part of internal control, and the resulting plans, programs or other actions deemed necessary by management to address the risks. The actions undertaken, as discussed in the prior paragraph, are a key part of the larger management process, but not an element of the internal control system.

As does ERM page 61:

Integration with Risk Response

Having selected risk responses, management identifies control activities needed to help ensure that the risk responses are carried out properly and in a timely manner.

In the current draft, Para 279 makes the distinction correctly:

279 Control activities are those actions that help ensure that responses to assessed risks, as well as other management directives, such as establishing standards of conduct in the Control Environment, are carried out properly and in a timely manner. For example, a company sets an operations objective "to meet or exceed sales targets for the ensuing reporting period," and management identifies a risk that the organization's personnel have insufficient knowledge about current and potential customers' needs. Management's response to address this identified risk includes developing buying histories for existing customers and undertaking market research initiatives to increase the organization's understanding of how to attract potential customers. Control activities might include tracking the progress of the development of the customer buying histories against established timetables, and taking steps to help ensure the quality of the reported marketing data.

The glossary also has the terms clearly identified:

- Control Activity—The actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

- Risk Response—The decision to accept, avoid, reduce, or share a risk

Comment 2: The use of a residual risk approach, whereby existing controls are identified then any additional risks are identified, should be highlighted as an effective Risk Assessment technique.

Para 242 establishes two types of risks to consider:

Inherent and Residual Risk

242 Management considers both inherent and residual risk. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management's response to inherent risk. Risk analysis is applied first to inherent risk. Once risk responses have been developed, as discussed below, management then considers residual risk.

In the vast majority of business situations, effective and efficient controls already exist. Asking evaluators or managers to perform inherent risk identification, including likelihood and impact estimations, when there are already controls in place is impractical. Trying to do this always results in inefficient and ineffective analysis of risks. The risks identified are either possible non-working controls, absent controls, impacts (not risks), or simply the opposite of the objectives. In my experience (from reviewing hundreds of risk matrix in QAR's, SOX efforts, ERM and internal audits) this one technique, inherent risk identification, has caused more confusion and effort than any other internal control tool – with no added benefit.

First identifying existing controls, then identifying any additional or remaining risks is far more efficient and effective, in practical application, and results in full identification of any risks that must be addressed. The question "What additional risks could occur, despite the controls already in place?" is the most important question in Risk Assessment, but is never asked using an inherent risk approach.

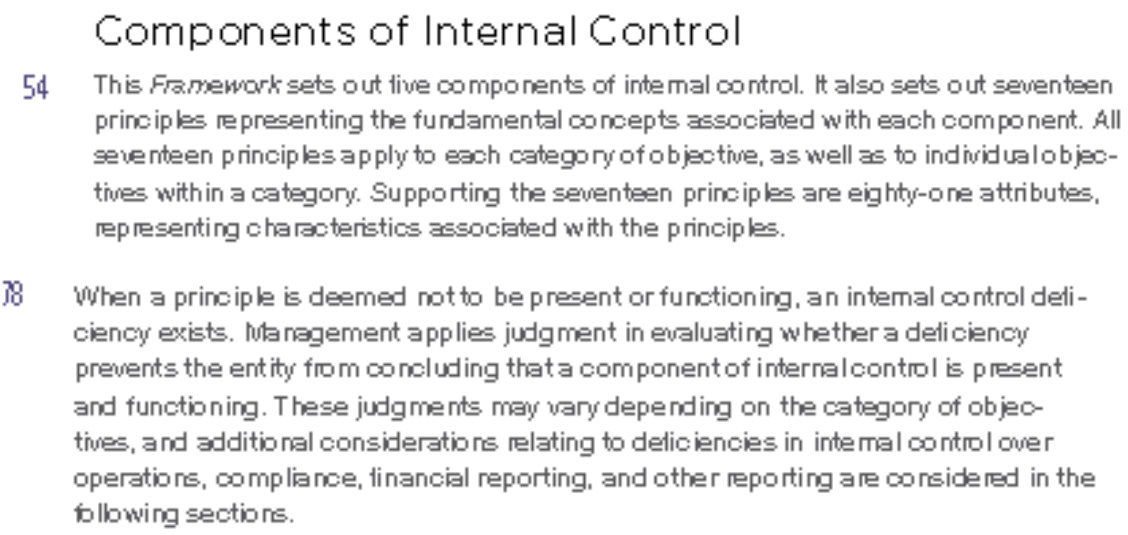
Para 249 establishes the possibility of using a residual risk approach, but the placement in the document is after inherent risks are identified, so not as useful or clear.

249 Resources always have constraints, and entities must consider the relative costs and benefits of alternative risk response options. Before installing additional procedures, management should consider carefully whether existing ones may be suitable for addressing identified risks. Because procedures may satisfy multiple objectives, management may discover that additional actions are not warranted or that existing procedures may be sufficient or simply need to be performed to a higher standard.

In my 20+ years of experience, this single issue (identification of inherent risks, despite and before considering the controls already in place) has directly led to the failure of many ERM, internal control and risk assessment workshops and efforts.

Comment 3 – Overly stress the requirement for all seventeen Principles of control to be applied.

The draft establishes seventeen principles within the five categories of control, as did the COSO guidance for smaller companies in 2006. All seventeen Principles are present in an adequately designed system of internal control, and all are operating effectively.



Components of Internal Control

54 This *Framework* sets out five components of internal control. It also sets out seventeen principles representing the fundamental concepts associated with each component. All seventeen principles apply to each category of objective, as well as to individual objectives within a category. Supporting the seventeen principles are eighty-one attributes, representing characteristics associated with the principles.

78 When a principle is deemed not to be present or functioning, an internal control deficiency exists. Management applies judgment in evaluating whether a deficiency prevents the entity from concluding that a component of internal control is present and functioning. These judgments may vary depending on the category of objectives, and additional considerations relating to deficiencies in internal control over operations, compliance, financial reporting, and other reporting are considered in the following sections.

In applying prior COSO publications (internal control, ERM, and small company), many (if not most users) have utilized only one tool, a risk matrix, to document controls. This tool typically results in the identification of a risk that precedes every control. This linkage of risks and controls is only the Risk Assessment Component of internal control (with additional information about management activities to respond to risks) – not the other four Components. Use of only a Risk Matrix tool (or the Risk Assessment and Control Activities Worksheet as called in the original COSO internal control Tools volume) results in a partial identification of controls, not controls in all seventeen Principles.

The current draft does not clearly portray that a matching of objectives, risks and controls is NOT present in all seventeen Principles, and will not correct the “partial” identification of controls many organizations now perform.

As a note, if all five Components of control are applied at an entity level, (rather than only the Risk Assessment Component) an inherent approach to risk assessment can work. However, as a risk matrix is the only tool used by most organizations, the inherent risk approach is impractical and not effective. (See Comment 2).

I will be pleased to answer any questions you may have.

Larry Hubbard
+1 (301) 529-8118
Larry@LHubbard.com