



KPMG LLP
757 Third Avenue
New York, NY 10017

Telephone 212-909-5600
Fax 212-909-5699
Internet www.us.kpmg.com

August 15, 2008

Dr. Larry E. Rittenberg
Chairman, Committee of Sponsoring Organizations of the Treadway Commission
4133D Grainger Hall, University of Wisconsin
975 University Avenue
Madison, WI 53706

Re: Guidance on Monitoring Internal Control Systems (June 2008)

Dear Dr. Rittenberg:

KPMG welcomes this opportunity to respond to the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) request for comment on its exposure draft, *Internal Control – Integrated Framework, Guidance on Monitoring Internal Control Systems* (Exposure Draft). We share COSO's belief that monitoring has been generally misunderstood and underutilized by many users of the COSO Framework. Accordingly, we support the issuance of further guidance to better describe the monitoring component of an effective internal control system.

Since the passage of the Sarbanes-Oxley Act of 2002, public companies have made significant investments to improve and enhance internal control over financial reporting. Guidance that assists organizations monitor whether those systems remain effective will not only improve the sustainability of those systems, but also improve the reliability of financial reporting and reports on internal control effectiveness. In addition, we believe that the guidance will enable organizations to improve the internal controls systems they maintain to meet operations and compliance objectives.

The remainder of this letter provides general observations and comments on the Exposure Draft. Specific comments regarding the contents of the Exposure Draft are included in the Appendices to this letter. Appendix A contains comments on Volumes I and II. Appendix B contains comments on Volume III.



Dr. Larry E. Rittenberg
August 15, 2008
Page 2

Is the Guidance an Addendum to the 1992 COSO Framework?

We believe further clarity about the relationship of the guidance to the 1992 COSO Framework is necessary in light of the widespread public reporting on internal control that identifies COSO as the criteria used to evaluate whether a system of internal control is effective. Clarity is important, not only for organizations implementing and evaluating their own monitoring, but also to enable users of internal control reports to better understand what guidance management considered in making their effectiveness assessment.

In this regard, we note that the Securities and Exchange Commission, in adopting its rules implementing the internal control evaluation and disclosure requirements of the Sarbanes-Oxley Act, explained that the use of standard measures for control effectiveness, such as the COSO Framework, were intended to, among other things, promote the comparability of the internal control reports of different companies. In the absence of clarity about whether the guidance is effectively an addendum to the 1992 COSO Framework, or a “best practices” document that does not contain guidance fundamental to the design and implementation of effective monitoring, COSO users may not use consistent criteria to define the monitoring component of the COSO Framework. To highlight this concern, it has been our experience that, in practice, and perhaps as result of the 2006 guidance being directed at smaller public companies, only the guidance associated with the 1992 COSO Framework is deemed to be ‘authoritative’ and considered by preparers in making public assertions.

The Exposure Draft makes a number of statements that the guidance ‘clarifies’ and ‘elaborates upon’ the 1992 COSO Framework, and that it will help users improve the ‘effectiveness’ of their monitoring function. Paragraph 2 of Volume I states that the guidance, “...elaborates on the monitoring component of internal control discussed in the 1992 COSO Framework and in the subsequent *Internal Control Over Financial Reporting - Guidance for Smaller Public Companies* issued in 2006.” It further states that the guidance “...does not change any of the fundamental elements of the COSO Framework or COSO’s 2006 Guidance.” Paragraph 4 of Volume II states that the Monitoring Guidance “...is intended to reinforce and clarify, not add to or change, the sound principles of monitoring previously established through the 1992 COSO Framework and COSO’s 2006



Dr. Larry E. Rittenberg
August 15, 2008
Page 3

Guidance.”¹ The Exposure Draft describes the objectives of the guidance as *i*) helping organizations improve the *effectiveness* (emphasis added) and efficiency of their internal control systems and *ii*) providing practical guidance that illustrates how monitoring can be incorporated into an organization’s internal control process. Volume II further explains that it is intended to help any organization “design, implement, and evaluate monitoring procedures that achieve the principles of the monitoring component.”

As a result of the foregoing, we recommend that COSO clarify those provisions of the guidance, if any, that are effectively an addendum to the 1992 COSO Framework. Further, we request that, if COSO determines that some or all of the guidance in Volumes I and II of the Exposure Draft should be characterized as optional or ‘best practices,’ then such guidance not be presented in a manner that implies adherence is necessary to achieve the objectives of monitoring.

Monitoring in an Internal Control System That Provides *Reasonable Assurance*

A more robust and clear discussion of the role of inherent limitations as they relate generally to internal control, and specifically to monitoring, will improve the final guidance by providing a clearer and more appropriate context for the judgments necessary to implement the guidance. To underscore the importance of this concern, we note that the Exposure Draft makes extensive use of imperative statements about monitoring and management actions in implementing it, and uses the terms “must,” “should,” and “enables,” to describe actions in implementing monitoring and the expected outcomes. In the Exposure Draft, reasonable assurance is discussed primarily as it relates to persuasive information, even though there are many other judgments made when implementing monitoring, many of which are impacted by the inherent limitations of internal control.

The Exposure Draft explains that the monitoring component is a process that evaluates the internal control system’s ability, in its entirety, to manage or mitigate meaningful risks, and describes its objective to include:

- enabling management and the board to determine whether the internal control system continues to operate effectively over time,

¹ Paragraph 2 of Volume II states that COSO’s 2006 guidance “further developed the understanding of how all five internal control components work cohesively to form an effective internal control system. Although targeted to smaller public companies... [it] contains information that should be helpful to all organizations, regardless of size... [the] 20 principles and supporting attributes clarify the COSO Framework so that organizations might apply [it] more effectively and efficiently.”



Dr. Larry E. Rittenberg
August 15, 2008
Page 4

- providing timely evidence of changes that have occurred, or might need to occur, in the way the internal control system addresses meaningful risks,
- leading to the identification and correction of control deficiencies *before* they materially affect the achievement of the organization's objectives, and
- requiring the evaluation of persuasive information.

It further explains that the implementation of monitoring requires judgments about matters such as the organization's tone at the top in relation to monitoring, the procedures necessary to have persuasive information about the operation of key controls, and the role of evaluators and their capabilities, objectivity and authority. We believe, subject to our other comments contained herein, that this guidance could be effective in enabling users to better understand the monitoring component of internal control and the nature of the judgments necessary to implement it. However, more clear explanations that these judgments are made within the inherent limitations of internal control would ensure that the context for the making these judgments is understood.

We also observed that Figure 2, *The COSO Monitoring Process*, in Volume II, illustrates the monitoring of the other four components to enable a determination of whether the objective of the system of internal control is met. However, the accompanying guidance does not effectively communicate that the inherent limitations of internal control apply to all five components, including monitoring. If the controls management implements to achieve the objectives of the other four components are designed at a level to provide reasonable assurance, the Exposure Draft may be misinterpreted as implying that the monitoring component will be implemented in a manner to provide absolute assurance that controls within other components operated as designed (i.e., to provide reasonable assurance). We believe revisions that clarify that implementation of monitoring is also subject to inherent limitations would improve the guidance.

Inter-relationship Between Risk Assessment and Monitoring

Understanding and Prioritizing Risks The Exposure Draft states that organizations "must determine what controls to monitor, what monitoring procedures to employ and how often to employ them," in order to implement effective monitoring. Paragraph 43 of Volume II states that, "designing monitoring begins with understanding and prioritizing the risks... [to identify] which are meaningful enough to subject to control monitoring." Paragraph 44 of



Dr. Larry E. Rittenberg
August 15, 2008
Page 5

Volume II further explains that risk prioritization is “a natural part of the risk assessment component” and that information from risk prioritization “influences decisions regarding the type, timing and extent of monitoring.”

We agree that risk assessment component activities provide helpful information about risks that is used to identify controls to monitor, and that such information will influence decisions about the nature of necessary monitoring procedures. However, we observe that the Exposure Draft provides guidance (paragraphs 50 through 53, and an associated ‘applying the concepts’ example) that is an incomplete description of risk assessment component activities. Moreover, the Exposure Draft uses phrases such as “might involve,” “might be,” and “might identify,” that may be misleading. We believe that guidance explaining the risk assessment component is unnecessary and that users of the guidance should be referred to other COSO risk assessment guidance (e.g., those referenced in footnote 18), which more completely describes risk assessment. Additionally, deleting the aforementioned risk assessment component guidance in the Exposure Draft will make the final document more concise overall and any incremental guidance on considerations specific to ‘monitoring’ (e.g., paragraph 54) more clear.

Change-Identification and Change-Management Processes The Exposure Draft contains a number of statements which explain that effective monitoring is implemented to ensure changes in risks and the operation of controls are identified timely and that such changes are properly managed by the system. For example, we observed the following guidance within the Exposure Draft:

- Paragraph 10 of Volume I states that, “...monitoring should (1) assess whether management reconsiders the design of controls when risks *change* (emphasis added).”
- Paragraph 21 of Volume I states that, “previously effective internal control systems become ineffective for one of two reasons: 1) the environment *changes* (emphasis added) without corresponding controls adjustments, rendering the existing controls unable to address new or altered risks, or 2) the operation of the internal control system *changes* (emphasis added) such that it no longer adequately manages or mitigates existing risks.”
- Paragraph 23 of Volume I explains that, “when ongoing-monitoring or separate-evaluation procedures identify a *change* (emphasis added) in the environment, the organization determines whether a corresponding change is needed in the internal control system. When monitoring identifies a *change* (emphasis added) in the internal



Dr. Larry E. Rittenberg

August 15, 2008

Page 6

control system, the organization needs to verify whether that *change* (emphasis added) was designed and implemented properly.”

- Figure 6, *Monitoring for a Change Continuum*, in Volume II, and the associated guidance in paragraphs 35 and 36, describe effective monitoring as being accomplished through *change-identification* and *change-management* processes applied to a “supported baseline of known effective internal control.”
- Paragraph 36 of Volume II states that, “effective change-identification and change-management processes provide important information to evaluators that influences their assessment of the risk that controls will fail to manage or mitigate risk (i.e., information about *changes* (emphasis added) that should be made in controls because the underlying processes or risks *change* (emphasis added), and information about *changes* in controls that have already taken place, such as *changes* (emphasis added) in personnel performing controls). As a result, change-identification and change-management processes can influence the scope of other monitoring procedures.”

We do not believe that the Exposure Draft adequately explains the change-identification and the change-management processes that are depicted in Figure 6, and discussed in the aforementioned sentences. The guidance on these processes, which appears mostly in Section II, *Establishing a Foundation for Monitoring*, is not well integrated with the remaining guidance in the Exposure Draft that explains designing and implementing monitoring procedures. Additionally, the Section II guidance appears incompatible with and contradictory to the model depicted in Figure 7, *Monitoring Design and Implementation Progression*, and the accompanying guidance included in Section III, *Designing and Executing Monitoring Procedures* (“Section III Guidance”). In this regard, we observed that the Section III Guidance provides no further discussion of these processes, even though Figure 6 and the aforementioned paragraphs describe the change-identification and the change-management process as consisting of ongoing-monitoring and separate-evaluations (i.e., monitoring procedures), and both processes as providing “important information to evaluators” and “warranting further discussion.”

To further illustrate our concerns, we note that paragraph 35.2 of Volume II explains that the risk assessment component of internal control identifies changes in processes or risks and verifies that the design of underlying controls remains effective, and that monitoring, through the use of ongoing monitoring and separate evaluations, should consider the risk assessment component’s ability to identify and address those changes. This paragraph further explains that monitoring also identifies *indicators of change* in the design or



Dr. Larry E. Rittenberg
August 15, 2008
Page 7

operation of controls and verifies that the controls continue to meet their objective of helping to manage or mitigate related risks. However, this guidance appears inconsistent with the Section III Guidance that describes how to design and implement monitoring procedures. Section III prescribes starting with output from the risk assessment component, and then using that information to identify controls to monitor and the information that will persuasively indicate whether the internal control system is *operating* effectively, and then implementing monitoring procedures to obtain the persuasive information. Because this guidance begins with output from the risk assessment component, it is not clear how this guidance would result in the design or implementation of ongoing-monitoring or separate evaluation procedures that provide persuasive information about the matters discussed in paragraph 35.2 of Volume II (i.e., the risk assessment component's ability to identify changes in processes or risks and verify that the design of underlying controls remains effective, or indicators of change in the design or operation of controls).

With regard to the change-management process, paragraph 35.3 of Volume II explains that "monitoring verifies" that the internal control system manages changes that occur in the operation of controls, or that are necessary in the design of controls. We observe that, for reasons similar to those above, the change-management process guidance also appears inconsistent with the Section III Guidance. We recommend that the guidance be revised to either delete the change-identification and change-management processes discussed in paragraphs 35 and 36 from the guidance, or more clearly integrate such guidance with Section III.

We also recommend that the guidance in Section III be revised to more clearly communicate how the model for designing and implementing monitoring presented therein considers the other four COSO components. In this regard, we note that paragraph 15 of Volume II explains that an "often overlooked" concept that [the COSO cube] demonstrates is that the components, including monitoring, operate at different levels across the organization (i.e., divisions, locations, processes, etc.), and that paragraph 26 of Volume II states that "[the COSO cube] demonstrates that individuals serving in different capacities within an organization may have some monitoring responsibility." This same concept applies to individuals involved in achieving the objectives of the other four COSO components (e.g., risk assessment), and we also believe that this concept is often overlooked. We recommend revising the guidance to clarify that the activities (i.e., controls) necessary to meet the objectives of other components of the Framework may exist at various levels of the organization, and that monitoring procedures should be implemented to consider the effectiveness of their operation.



Dr. Larry E. Rittenberg
August 15, 2008
Page 8

Lastly, we recommend the guidance be revised to provide a more thorough and clear explanation of how all four components operating at different levels (i.e., divisions, locations, processes, etc.) across the organization are considered when understanding the internal control system and identifying important controls to monitor (i.e., key controls) and that the guidance on identifying persuasive information be revised to more clearly address its application to the nature of activities and types of controls that are implemented to achieve the objectives of the other components.

Definition of Key Controls

The Exposure Draft provides guidance on which controls should be monitored to meet the objective of the monitoring component. It refers to such controls as “key controls,” and defines them in the Glossary as “those controls that are *most important* (emphasis added) to monitor in order to support a conclusion about the internal control system’s *ability* (emphasis added) to operate effectively and which often have one or both of the following characteristics: i) their failure might materially affect the organization’s objectives, yet not reasonably be detected in a timely manner by other controls, and/or ii) their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the organization’s objectives.” We provide the following three comments with respect to this definition of key controls.

We believe that this definition is inconsistent with the purpose of monitoring in a system that provides reasonable assurance that an organization’s objectives will be met. The second characteristic states that a control whose operation “might” prevent other failures or detect such failures would be considered a key control. The word “might” connotes *any* possibility of preventing or detecting failures in other controls. A key control must be able to prevent or detect failure in another control at a high level of assurance, particularly if the “other” controls relate to risks that could materially affect the organizations objectives. In this regard, we note that the 1992 COSO Framework states that “monitoring *ensures* (emphasis added) that internal control continues to operate effectively.”

Additionally, and as explained more fully in Appendix A to this letter, the use of the phrase “most important to monitor” states that someone could monitor something less than all of the controls that are necessary to support a conclusion. For example, one could determine that monitoring only the *most important* ten-percent of controls necessary to support a



Dr. Larry E. Rittenberg
August 15, 2008
Page 9

conclusion about the internal control system's ability to operate effectively is acceptable.

Lastly, we note that the objective of monitoring is to determine *whether* the internal control system 'continues to operate effectively,' not just its *ability* to do so.

We recommend that the final guidance be revised to address the matters discussed above.

Drafting Style

The vast majority of entities that report on the effectiveness of their internal control system refer to the COSO Framework. As such, the clarity of the guidance and the ability for it to be consistently understood and applied by a wide constituency is of paramount importance. Guidance that lacks clarity or is overly prescriptive may not be effectively implemented by the widely diverse organizations that use COSO, and may have the unintended consequence of worsening, rather than improving, the effectiveness and efficiency of monitoring.

Regardless of whether COSO concludes that the guidance represents an addendum to the 1992 COSO Framework or an optional 'best practices' tool, guidance that is clear, and which users can effectively implement, is critical. Guidance that represents "best practices" or "an approach" for implementing monitoring and is published by COSO, may give rise to a 'rebuttable presumption' that it describes what COSO believes is effective monitoring under the COSO Framework. As a result, users that choose to pursue an alternative approach may feel pressure to reconcile or justify their own approach with the 'best practices' guidance. Therefore, clear articulation of the matters about the nature of judgments that were made and why such approach was deemed by COSO to be appropriate remain essential to the publication of this guidance. Accordingly, we believe that COSO should take whatever steps are necessary to ensure that the final document is sufficiently clear and capable of being effectively implemented by the wide variety of organizations that report on internal control.

As discussed elsewhere in this letter, we believe that effective implementation of monitoring requires significant judgment. A corollary to this is that any "guidance" for doing so should serve to articulate clearly the conceptual elements COSO believes are essential to achieving the objective of monitoring, and the nature of judgments that users of the guidance should make.

We believe that the Exposure Draft contains opportunities to improve the clarity, concision, and internal consistency of the guidance and reduce the likelihood of significant questions



Dr. Larry E. Rittenberg
August 15, 2008
Page 10

and uncertainty on the part of COSO users arising after its issuance in final form. We have included specific comments in the Appendices to this letter of guidance that we recommend be considered for revision. In summary, these comments include recommendations to:

- Avoid the use of words such as “any,” and “all,” when they connote unnecessary definitiveness, and “most,” “many,” “some,” and similar words when they connote a degree or measure that is ambiguous. The use of such words in other widely used guidance has led to implementation issues and may ultimately restrict the degree of judgment exercised.
- Avoid the use of adjectives and modifiers that are unnecessary, or for which the context is not fully explained. For examples, phrases like “*perhaps* extensive” or “*supported* understanding” are not clear because the context is not present in the guidance to effectively communicate what COSO intends by their use.
- Ensure that the guidance makes clear the intended difference in meaning when terms such as ‘must,’ ‘should’ or present tense statements are used to describe what the implementation of monitoring involves.
- Further reduce the use of examples within the text of the guidance itself. We observed that the Exposure Draft’s use of examples within the guidance itself, as opposed to the ‘applying the concepts’ sections, often add unnecessarily to the length of the guidance. The guidance itself should be sufficiently clear to ‘stand on its own.’ In some situations it appears the examples are provided to clarify what is otherwise incomplete or ambiguous guidance.

* * * * *



Dr. Larry E. Rittenberg
August 15, 2008
Page 11

We support COSO's efforts to provide additional guidance on monitoring of internal control, and we appreciate the opportunity to provide comments on the Exposure Draft. If you have any questions regarding information included in this letter, please do not hesitate to contact Craig W. Crawford, (212) 909-5536, ccrawford@kpmg.com.

Very truly yours,

KPMG LLP

cc: Mr. Conrad Hewitt, Chief Accountant – SEC
Mr. Thomas Ray, Chief Auditor and Director of Professional Standards – PCAOB



Dr. Larry E. Rittenberg
August 15, 2008
Page 12

Appendix A

Guidance on Monitoring Internal Control Systems (June 2008)

The following specific comments related to Volume I and II are presented for consideration:

Monitoring to “Assess” or “Verify”

Paragraph 10 of Volume I states that “...monitoring should (1) *assess* (emphasis added) whether management reconsiders the design of controls when risks change, and (2) *verify* (emphasis added) the continued operation of existing controls that have been designed to reduce risks to an acceptable level” and that COSO “...[believes] monitoring should be based on a *fundamental analysis* (emphasis added) of risks and an understanding of how controls may or may not manage or mitigate those risks.”

The use of the term “assess” to state that monitoring considers whether the design of controls was reconsidered and the term “verify” to state that monitoring considers the continued operation of controls connotes to a user of the guidance that COSO intends a different meaning for each. We observe, however, that there is no additional guidance in the Exposure Draft that explains COSO’s intent with the use of these words. We recommend that the final guidance avoid use of language in an ‘executive summary’ that does not also appear, or is not clearly cross-referenced to, guidance that appears in Volume II. Additionally, we recommend that the final guidance replace the words “assess” and “verify” in the aforementioned sentence with the word “evaluate.” We believe “evaluate” will more effectively communicate that implementation requires the use of judgment, as appropriate in the circumstances, to form monitoring conclusions.

The use of the term “fundamental” to describe the analysis of risks upon which monitoring is based, communicates that COSO believes a risk analysis with particular characteristics is necessary. However, the Exposure Draft does not explain the characteristics COSO intends with the use of ‘fundamental’ analysis of risks or contrasts it with another approach. We recommend revising the guidance to clarify what COSO intends or deleting the word “fundamental” from phrase “fundamental analysis of risks.”

The Frequent Use of “Most” in the Guidance

Throughout Volume I and II the guidance repeatedly uses the term “most” in ways that either do not enable a user to better understand the principles and concepts underlying



Dr. Larry E. Rittenberg
August 15, 2008
Page 13

monitoring or otherwise obfuscates their meaning. The use of “most” in the Exposure Draft does not, in our view, promote a better understanding of monitoring. Furthermore, it detracts from the “neutrality” of the document by establishing a bias as to what the outcome of a user’s judgments should be. If, in fact, COSO intends its use to direct users to implement monitoring that is consistent with what is described in the Exposure Draft as ‘most effective,’ such intention is not transparent from the guidance.

The use of “most” in drafting the guidance increases the risk that users will not be able to understand the guidance or exercise the judgment necessary to apply it effectively. We observe that “most” is commonly understood to mean ‘the majority of’ something or ‘existing in the greatest quantity, number or degree.’ Its use in the Exposure Draft to describe COSO’s observations about the frequency of practices employed or conclusions reached is done without sufficient context or explanation. For example, its use in the Exposure Draft does not provide enough information to allow a user to evaluate whether it means substantially all (e.g., 95%), a slight majority (e.g. 51%) or just the single largest common set (e.g., 35% with no other practice or conclusion representing more than 35%) of the observed instances that serve as COSO’s basis for the generalized “most” statement. Additionally, the guidance does not contain information about the population of organizations upon which the generalizations were drawn. Similar problems arise when the guidance uses “most” to describe the degree to which an objective is achieved, or the comparative relevance of something in doing so (e.g., ‘most effective’ or ‘most important’). The lack of context about the degree of effectiveness or the relative importance of other factors, which are generally not described or explained, limits the usefulness of the guidance and may have the practical effect of creating “definitions” of what is required when the intent of COSO is to not do so.

The following paragraphs provide examples of where we believe usefulness of the guidance would be improved by eliminating the word “most” and more clearly explaining the concepts and reasons as to why “most” was used in the Exposure Draft. We also have provided additional comments and observations to further explain our concerns and recommendations.

- *Paragraphs 17 of Volume I and 24 of Volume II* - In **most** cases, the board is ultimately responsible for determining whether management has implemented effective internal control (including monitoring).

We observe that this statement implies that there are situations where the board would not be responsible for the effectiveness of monitoring. We believe the usefulness of the



Dr. Larry E. Rittenberg
August 15, 2008
Page 14

guidance would be improved by explaining when COSO believes such situations would exist.

- *Paragraphs 28 of Volume I and 46 of Volume II* - Important controls — often referred to as key controls — are those that are **most** important to monitor in order to support a conclusion about the internal control system’s ability to operate effectively.

The use of the phrase “most important to monitor” states that someone could monitor something less than all of the controls that are necessary to support a conclusion. For example, one could determine that monitoring only the *most important* ten-percent of controls necessary to support a conclusion about the internal control system’s ability to operate effectively is acceptable.

- *Paragraph 62.9 of Volume I* - **Most** organizations will use a combination of both approaches, but ongoing-monitoring using appropriately persuasive information is often **most** effective and efficient.

We recommend minimizing the use of phrases such as “most effective” as they may be understood to imply a necessary action or outcome, when, in fact, users only need to establish monitoring that is “effective.”

- *Paragraph 10 of Volume II* - Monitoring is **most** effective and efficient when it considers how the *entire* internal control system manages the risks to achieving the organization’s objectives. In contrast, it is **less** effective and efficient when it focuses on a checklist of control activities that are selected for evaluation without regard to (1) the level of the risk they address, or (2) their relative importance in addressing the risk.

Similar to the previous bullet, we recommend minimizing the use of phrases such as “most effective” as they may be understood to imply a necessary action or outcome, with alternatives potentially being construed as sub-standard even though the alternative may be effective. Additionally, the use of the phrase “less effective” has the connotation of that which is *not* effective, when, in fact, it may be effective in the circumstances.

- *Paragraph 22 of Volume II* - Monitoring operates **most** effectively when (1) the roles and responsibilities of management and the board regarding monitoring are appropriate and clearly articulated, and (2) evaluators with proper characteristics are placed in the right positions.



Dr. Larry E. Rittenberg
August 15, 2008
Page 15

The use of “most” in this example suggests that clear and appropriate monitoring roles for management and the board, or the use of evaluators with appropriate characteristics are not necessary for effective monitoring. If COSO believes their presence is not necessary, we recommend the guidance be revised to clarify when the presence of such matters is not necessary.

- *Paragraph 56 of Volume II* - Key controls might include those that represent the **most** likely point of failure regarding meaningful risks.

We believe an adequate understanding of this statement requires additional explanation as to when a control that represents “the most likely point of failure regarding meaningful risks” would *not* be considered a key control.

We recommend that the guidance be revised to explain the underlying concepts and reasons as to why, in fact, “most” is a relevant descriptor. As stated elsewhere in this document, we believe that the drafting style of the final guidance must provide clear and concise descriptions of the concepts and factors to consider in implementing monitoring procedures that are consistent with the objectives of the COSO Framework. Doing so will enable users to use judgment to implement monitoring that is appropriate in their particular circumstances more effectively than if the drafting style of the Exposure Draft is retained.

Control Baseline Guidance

A Control Baseline that is Perhaps Extensive The Exposure Draft uses the word “perhaps” to describe whether an initial baseline understanding of risks and controls needs to be “extensive.” Paragraphs 20 of Volume I and 35 of Volume II state that, “if an organization does not already have such a baseline understanding in an area with meaningful risks, it will need to perform an initial, and *perhaps extensive* (emphasis added), evaluation of the design of internal control and determine whether appropriate controls have been implemented.” We recommend that the final guidance eliminate the phrase “and perhaps extensive.” Without an expansion of the guidance to explain factors relevant to judgments about the need to vary the “extensiveness” and how a user might do so, the “perhaps extensive,” terminology is not helpful.

We believe that the guidance should be drafted with the presumption that users will, on their own accord and without reminder, establish the understanding that is, in fact,



Dr. Larry E. Rittenberg
August 15, 2008
Page 16

appropriately extensive in the circumstances. Guidance that the extensiveness of the understanding should vary without establishing any context or elaboration on what is meant by “extensive” provides little benefit to users.

A Control Baseline Understanding that is “Supported” Paragraphs 20 of Volume I and 35 of Volume II state that “monitoring starts with a *supported understanding* (emphasis added) of the internal control system’s design and of whether controls have been implemented to accomplish the organization’s internal control objectives.” We recommend that the final guidance eliminate the word “supported.” Without an expansion of the guidance to explain what COSO means by a “supported” understanding or the nature of activities necessary to establish such an understanding, we believe that the use of the word is not helpful.

Similar to our comment above, we do not believe that the word “supported” will effectively reduce the risk that users will implement ineffective monitoring because they do not understand their existing controls.

The Meaning of “Environment”

The Exposure Draft makes repeated references to “environment” and changes therein when describing what monitoring should consider. For example, paragraph 34 of Volume II, states that “...changes in the *external environment* (emphasis added) or in the manner in which internal control systems operate create risks to the organization’s objectives that the internal control system may fail to manage.” Paragraph 69 of Volume II, states that “...indirect information can be a valuable monitoring tool that may...signal that a change in the *environment* (emphasis added) or control operation has occurred.”²

The Exposure Draft does not elaborate on, or otherwise explain, what COSO means when making reference to the “environment” or “external environment.” Paragraph 54 of Volume II describes three categories of “risk factors” to consider when designing and implementing monitoring procedures: *i*) nature of operations, *ii*) *environmental* (emphasis added) factors and *iii*) susceptibility to theft or fraud. Even though only one category is called “environmental”, we believe that the definitions the Exposure Draft provided for each of these three categories should apply when the guidance discusses monitoring for changes in the “environment” or “external environment.”

² Other examples not cited here include paragraphs 21, 22 and 23 of Volume I and 51 and 54 of Volume II.



Dr. Larry E. Rittenberg
August 15, 2008
Page 17

The Interval between Separate Evaluations

The guidance uses the phrase “as the potential impact and/or likelihood of *a control’s failure* (emphasis added)” in Paragraph 43 of Volume I and the phrase “likelihood and significance of *the risk’s occurrence* (emphasis added)” in paragraph 87 of Volume II to describe the interval between separate evaluations. We do not believe these phrases will be interpreted to have the same meaning. We note that phrase in paragraph 43 appears to describe the likelihood that the control system will fail to properly manage or mitigate a given risk (e.g., see the factors in paragraph 58 of Volume II), which is different than the likelihood and significance of the occurrence of the underlying risk for which controls were implemented. We recommend that the final guidance be revised to clarify these sentences.

Role of Persuasive Information in Effective Monitoring

Paragraph 32 of Volume I states that “...monitoring *must* (emphasis added) evaluate a sufficient amount of suitable information” to be effective. Paragraph 78 of Volume II states that “evaluators must gather sufficient suitable information to support a reasonable conclusion about control effectiveness.” Paragraph 40 of Volume II states that organizations “...*must* (emphasis added) determine three things [to] implement monitoring that provides the necessary level of support: *i*) what controls to monitor, *ii*) what monitoring procedures to employ, and *iii*) how often to employ them.”

We observe the above statements, which use “must” to describe actions necessary for effective monitoring, appear only within Section III of Volume II. The Exposure Draft does not use the word “must” to describe any of the concepts presented in Section II, *Establishing a Foundation for Monitoring* or in Section IV, *Assessing and Reporting Results*. It is not clear from the Exposure Draft whether this was done intentionally to emphasize that COSO believes “persuasive information” is more important to effective monitoring than concepts such as the competence and objectivity of evaluators or the prioritizing and reporting of monitoring results. We believe that concepts set forth in Sections II and IV also contain monitoring concepts that are equally important to its effectiveness.

We recommend that the guidance be revised to not use the phrase “must” only in connection with persuasive information. In this regard, we believe that using “should” to describe the aforementioned items relating to persuasive information would make the guidance more consistent with that which appears in Sections II and IV and ensure that



Dr. Larry E. Rittenberg
August 15, 2008
Page 18

users appropriately consider all of the concepts presented in the guidance in implementing monitoring.

Competence and Objectivity Considerations of Evaluators

Paragraph 28 of Volume II states that “competence and objectivity considerations help organizations determine *who should perform monitoring procedures* (emphasis added).” However, the description in paragraph 25 of Volume II states that “evaluators” consist of “...people who are responsible for determining what and how to monitor, assessing the monitoring information, and reaching a conclusion regarding the effectiveness of internal control.” This gives rise to an apparent discrepancy in the guidance because it is not clear whether the reference in paragraph 28 to those who “perform monitoring procedures” is intended to be to those “responsible for assessing monitoring information” or instead, is referring to the individuals discussed in paragraph 27 of Volume II who are not “evaluators,” but who “do produce information the evaluators use to reach their final conclusions.” We recommend the final guidance be revised to clarify this distinction.

We also observed that the statement below from Paragraph 83 is unclear as to whether the ‘people performing’ the separate evaluations or ongoing-monitoring are ‘evaluators’ or “persons that produce monitoring information.” We recommend the following revisions to the guidance under the presumption that COSO intends that “people performing” are *evaluators*.

Separate evaluations are often performed by ~~people~~ evaluators who are not ~~directly~~ responsible for the operation of the controls being monitored. As such, they may provide other evaluators a more objective analysis of information about control effectiveness than ongoing-monitoring procedures that are often performed by less and promote the objectivity of objective personnel who provide the information to evaluators in ongoing-monitoring procedures.

Persuasive Information Guidance

Monitoring Requires Information that “Is Persuasive” and Not “Less” or “More” Persuasive Paragraph 59 of Volume II defines persuasive information as that which gives the evaluator “reasonable, but not necessarily absolute, support for a conclusion regarding the continued effectiveness of the internal control system in a given risk area.” This notion of persuasive information is not a judgment made on a continuum or sliding scale for which



Dr. Larry E. Rittenberg
August 15, 2008
Page 19

there is a need for a concept of “degree” of persuasiveness. We agree that the characteristics of monitoring information that is deemed persuasive may vary based on the nature of the underlying risks and controls. However, the Exposure draft uses the phrase “less-persuasive” and “more-persuasive” to refer to information that, in fact, is *not* persuasive. We believe that references to information that is *not* persuasive as being “less-persuasive” or “more-persuasive” will lead to confusion and the misapplication of the guidance. Further, we observe that the references to “degrees of persuasiveness” can be eliminated without significant revisions to, or expansion of, to the guidance contained in the exposure draft. In this regard, we provide the following suggested revisions:

- First sentence of Paragraph 59 of Volume II - ~~The p~~Persuasiveness of information refers to the degree to which the monitoring information is capable of providing adequate support for a conclusion regarding the effectiveness of internal control.
- Last sentence of Paragraph 59 of Volume II - Regardless of the method, determining the information necessary level of persuasiveness to have reasonable, but not necessarily absolute, support for a conclusion regarding the continued effectiveness of the internal control system in a given area requires those responsible for monitoring to exercise judgment.
- Second sentence of sub-bullet 4 of Paragraph 35 of Volume II - When ongoing-monitoring uses ~~less-persuasive~~ information that is, by itself, not persuasive, or when the level of risk warrants, monitoring periodically revalidates control operation through separate evaluations using ~~appropriately~~-persuasive information.
- First and second sentences of Paragraph 88 of Volume II - The ~~level of persuasive~~ information used in ongoing-monitoring procedures can also influence the frequency of separate evaluations. Ongoing-monitoring that evaluates ~~more-persuasive~~ information in a given risk scenario might provide all the support necessary to conclude on the effectiveness of the internal control system in that area.

The second sentence of Paragraph 88, which is included above, illustrates how the use of degrees of persuasiveness language in the Exposure Draft may be misunderstood. This sentence literally states that ‘all the support necessary to conclude on effectiveness’ can come from information that is “more-persuasive” than some other information. It does not clearly state that the information used by the ongoing-monitoring *is persuasive*, as is required by the Exposure Draft. Similarly, the second sentence of sub-bullet 4 of paragraph



Dr. Larry E. Rittenberg

August 15, 2008

Page 20

35 explains that information that is “less persuasive” needs to be revalidated through separate evaluations and thereby implies that it is, in fact, not persuasive.

We recommend that the term “persuasiveness of information” be deleted from the final guidance and that references to “more-persuasive” or “less-persuasive” be deleted and redrafted with alternative language as suggest above.

Clarity of Definitions of Direct and Indirect Information The Exposure Draft uses a model of “direct” and “indirect” information to explain the relevance of monitoring information. Paragraph 65 of Volume II states that information which “*directly confirms* (emphasis added) the operation of controls is more relevant than information that merely allows the evaluator to infer whether the controls are working.” We observe that the discussion of direct information in the Exposure Draft uses inconsistent language among Volumes I and II and the Glossary. In addition, the meaning COSO intends with the use of certain terms and phrases is not clear in the Exposure Draft. We provide the following specific comments for your consideration.

- The language that describes the defining attribute of direct information is not clear. For example:
 - Paragraph 65 of Volume II uses the phrase “information that *directly confirms* (emphasis added) the operation of controls,”
 - Paragraph 66 of Volume II uses the phrases “direct information *substantiates* (emphasis added) the operation of controls” and “*provides an unobstructed view* (emphasis added) of control operation,” and
 - The Glossary uses the phrase “information that *directly substantiates* (emphasis added) the operation of controls.”

We recommend that the final guidance be revised to clearly describe the defining characteristics of “direct information” using the same language throughout. Furthermore, we recommend that the guidance clarify that *i*) direct information *explicitly demonstrates*,³ for the instances (or period of time) to which the direct information relates, whether or not a control operated in a manner consistent with its

³ We note that the definition of indirect information explains its defining characteristic as the inability to ‘explicitly’ demonstrate a control’s operation.

design, and *ii*) evaluators then evaluate the direct information and use judgment to arrive at conclusions about effectiveness.

- The guidance on direct information in paragraphs 33 of Volume I and 66 of Volume II, which states that, “generally, direct information is highly *relevant* (emphasis added). . .” is inconsistent with that which appears in the Glossary and states that “direct information is generally highly *persuasive* (emphasis added).” We recommend that the guidance in the Glossary be revised to use “relevant” as is done in paragraphs 33 of Volume I and 66 of Volume II.
- Paragraph 15 of Volume II explains that “as organizations increase in size, evaluators at the highest organizational levels — who are removed from *direct* (emphasis added) interaction with controls or process owners — often monitor by evaluating the results from monitoring activities performed at another level.” We believe that the final guidance should clarify that, for purposes of the *relevance* of monitoring information, the determination of whether it is *direct* or *indirect* is based upon how the information was generated. For example, a conclusion that is based on direct information of an evaluator at an account or process level, which is then communicated upward through the organization, is still considered highly ‘relevant’ (i.e., the attribute associated with direct information) as it is used by evaluators at successively higher levels. Absent such clarification, the guidance may be misunderstood to suggest that monitoring information, which was considered “direct” at an individual account or process-level, may become “indirect” simply by virtue of having evaluators at multiple-levels use the conclusions of an evaluator at the account or process-level.

Clarify Objectivity Considerations With Regard to Information Reliability Paragraph 73 of Volume II states that “reliable information is accurate, verifiable, and *comes from an objective source* (emphasis added).” Paragraph 75 of Volume II states that objectivity, for purposes of the source of information (i.e., as opposed to objectivity of evaluators who use that information), “. . . is the degree to which that source can be expected to provide unbiased information for evaluation.” It goes further to explain that the more objective the information source, the more likely the information will be reliable.

We observe that this guidance appears inconsistent because the statement that ‘reliable information comes from an objective source’ does not connote degrees of objectivity contemplated in Paragraph 75. We recommend the statement in paragraph 73 be revised to clarify the notion of degrees of objectivity by stating that “comes from an *appropriately* objective source.” Furthermore, we recommend that the guidance clarify that judgments



Dr. Larry E. Rittenberg
August 15, 2008
Page 22

about whether either an evaluator or source of information is appropriately objective, considers both factors that may *inhibit* or *promote* a person's ability to perform with the necessary degree of objectivity.

Furthermore, we recommend deleting the sentence in paragraph 75 which states that "notifying information sources in advance that certain instances of a control will be monitored, or directing them to provide supporting documentation in such a manner and time frame that they have an opportunity to review and correct that documentation before it is examined, reduces the information's objectivity and, therefore, its reliability." As drafted, this guidance may unduly limit the manner in which evaluators seek to obtain monitoring information. We recommend replacing it with a more principles based statement that simply explains that evaluators should consider whether the manner in which monitoring information requests are made increases the risk that the information's objectivity is reduced and take appropriate measures to eliminate or mitigate that risk.

Other Guidance

The following comments describe guidance contained in the Exposure Draft that we believe should be considered for revision to improve the clarity of the guidance.

- *Paragraph 10 of Volume I* – The use of the word "help" in the phrase "help ensure" is inconsistent with the COSO Framework. The COSO Framework states that "monitoring *ensures* (emphasis added) that internal control continues to operate effectively." We recommend the guidance in this paragraph be revised as follows:

~~No~~ A system of internal control can guarantee can only provide reasonable, not absolute, assurance regarding the prevention and detection of all control deficiencies that result in the inability to achieve organizational objectives. However, when properly designed and executed, monitoring will help ensure that internal control continues to operate effectively.

- *Paragraph 22 of Volume II* – We believe the usefulness of the guidance would be enhanced by a more thorough explanation of the roles and responsibilities of the board and management as it relates to monitoring, and that the emphasis on 'clearly articulated' is unnecessary. We recommend the guidance in this paragraph be revised as follows:



Dr. Larry E. Rittenberg
August 15, 2008
Page 23

Monitoring involves establishing appropriate ~~operates most effectively when (1) the roles and responsibilities of management and the board regarding monitoring are appropriate and clearly articulated, and (2) placing~~ evaluators with proper characteristics ~~are placed in the right~~ appropriate positions.

- *Paragraphs 16 of Volume I and 23 of Volume II* – The use of the phrase “makes sure” in these paragraphs is unnecessary, inconsistent with other terminology in the guidance, and unclear in relation to the use of the phrase “ensure” in the 1992 COSO Framework. We recommend the guidance in this paragraph be revised as follows:

Management establishes the system and ~~makes sure that~~ implements monitoring to ensure that it continues to operate effectively.

- *Definition of Information and Communication in the Glossary of Volume II* – The phrase “nerve-center function” within the below sentence is colloquial and unclear, and therefore provides little benefit as guidance. We also observe that it was not in the 1992 COSO Framework. We recommend that the sentence be deleted from the guidance.

~~Information and communication refer to the nerve-center function of an internal control system.~~

- *Paragraphs 44 of Volume I and 95 of Volume II* – The guidance states that the results of monitoring ‘are compiled,’ but does not elaborate on what COSO means. If there is a specific type of compilation activity that COSO believes is necessary, we recommend that the final guidance be revised to include it. Otherwise, we believe that stating that the results are to be reported is sufficiently clear and makes the notion of “compiled” extraneous. We recommend the guidance in these paragraphs be revised as follows:

The monitoring process ~~is complete when~~ ensures that the results of monitoring are ~~compiled and~~ reported to appropriate personnel. This ~~final stage~~ enables the results of monitoring to either confirm previously established expectations about the effectiveness of internal control or highlight identified deficiencies for possible corrective action.

- *Paragraph 101 of Volume II* – We recommend that the guidance in this paragraph be revised as follows to clarify its meaning and usability:



Dr. Larry E. Rittenberg
August 15, 2008
Page 24

~~In any case (except, perhaps, where fraud is suspected), control~~ Control deficiencies should be reported to the person directly responsible for the control's operation and to management that has oversight responsibilities and is at least one level higher.

- *Paragraph 55 of Volume I* – The guidance states that, “...*implicit* (emphasis added) knowledge about the operation of internal control may allow the evaluator in a smaller organization to support his or her control conclusions through *less-intensive* (emphasis added) monitoring...” We believe the guidance should be expanded to more clearly differentiate ‘implicit’ knowledge from ‘explicit’ knowledge and how each applies in contrast to a large and small organization. Absent clarification, one could reason that the knowledge about control operation held by senior management in a smaller organization would be based more on actual first hand knowledge (i.e., which seems more ‘explicit’) given their close proximity to the operation of controls. Moreover, we recommend that the guidance clarify what is meant by “less-intense” monitoring because there is not a common understanding of such a term or how it would be applied within the context of the concepts set forth in the Exposure Draft.
- *Paragraph 92 of Volume II* – The guidance discusses the role of automated computer monitoring tools. We recommend that this guidance be expanded to emphasize that the integrity and reliability of such IT-based monitoring tools is dependent on the effectiveness of certain IT general controls (e.g., logical access and program change controls). Additionally, the exposure draft makes only brief references to what humans actually do with exception data and other outputs of system-based monitoring. We believe that this important concept should be emphasized. We suggest adding a broad statement that automated capture and reporting of exception data is insufficient on its own in situations where appropriate review and follow-up are a necessary component of such monitoring.



Dr. Larry E. Rittenberg
August 15, 2008
Page 25

Appendix B

Guidance on Monitoring Internal Control Systems (June 2008)

The following specific comments related to Volume III are presented for consideration:
Section II – Establishing a Foundation for Monitoring

- Example 5 in the subsection related to Organizational Structure provides an example of “Use of a formal risk committee to develop and communicate expectations.” The last sentence of the example states, “As a result, management has a “road map” in which financial and operational controls in the business are linked to the risks identified during the annual risk assessment”. It is not clear how this example meets the objective that expectations are communicated. We recommend clarifying or expanding the example in this regard.
- Example 22 of the subsection related to Identify Persuasive Information provides an example of “Use of indirect information in addressing operational risks.” This example states that “Management may initiate a specific quality audit (i.e., separate evaluation) of any process where statistical indicators show a negative trend or where it identifies, through observation or customer complaint, a potential quality issue”. We believe that the guide should clarify how the timing and nature of the separate evaluations sufficiently reduces the likelihood of not meeting the entity’s objective.
- Example 30 of the subsection related to Using Technology for Effective Monitoring provides a “Continuous monitoring of segregation-of-duties controls” example that explains a segregation-of-duties tracking tool that “produces a report listing all [segregation of duties] conflicts that meet predefined criteria, which is reviewed by appropriately objective personnel.” We recommend the example clarify how the objectivity and competency of the personnel reviewing the conflicts identified by the segregation of duties (i.e., the evaluator) was considered.
- Examples 39 and 40 of the subsection related to Reporting Internally provide examples of “Established reporting protocols for identified deficiencies” and “Use of a spreadsheet to track and report deficiencies.” Both examples contemplate the tracking and communication of identified control deficiencies; however, the examples do not address remediation steps undertaken to address the deficiencies before they materially affect the organization’s objectives. We suggest that the examples clarify this consideration.



Dr. Larry E. Rittenberg
August 15, 2008
Page 26

Section V – Comprehensive Examples – Monitoring of Controls over Certain Operational Risks in a Mid-Sized Manufacturing Organization

- Paragraph 5 of the subsection related to Monitoring of Controls over Certain Operational Risks in a Mid-Sized Manufacturing Organization provides an organizational chart where the internal audit department reports to the Chief Financial Officer. We recommend that the discussion address how an internal audit department not reporting to the audit committee may impact its objectivity as evaluators.

Section V – Comprehensive Examples – Monitoring Certain Information Technology (IT) Controls

- Paragraph 3 of the subsection related to Monitoring Certain Information Technology (IT) Controls discusses “Understanding and Prioritizing Risk.” In the Example Factors Influencing Risk Prioritization for the risk area related to inappropriate access, we recommend that you consider adding the complexity of the computing environment. This factor has a significant effect on the risk of inappropriate access. In addition, we recommend that the discussion on the example factors influencing risk prioritization related to program integrity be expanded to recognize that modified package software exists on a continuum with various shades of customization and configuration (e.g., package systems are often customized more and more over time, and they slowly morph from packaged to highly customized in small increments).
- Paragraph 4 of the subsection related to Monitoring Certain Information Technology (IT) Controls states that, “at times monitoring manual controls can provide sufficient support for a conclusion regarding the effectiveness of IT controls that operate earlier in the transaction process.” We suggest that you revise the guidance to clarify that such monitoring may obviate the need to rely on such IT controls to support evidence around financial reporting or other objectives. The conclusion therefore relates to those objectives, not to the effective operation of the complementary IT controls themselves.
- Paragraph 5 of the subsection related to Monitoring Certain Information Technology (IT) Controls includes a table that summarizes IT controls that are generally important. We suggest adding the following key controls:



Dr. Larry E. Rittenberg
August 15, 2008
Page 27

- The periodic management review of access rights as a key control in the row for Data Security & Change Control.
 - Problem and incident monitoring and resolution as a key control in the row for Job Scheduling & Management.
- In paragraph 5 of the subsection related to Monitoring Certain Information Technology (IT) Controls, we suggest rewording the description under the table row for Security Log Monitoring as follows: “A common control in any IT environment is the unique identification and authentication of users. This is typically accomplished by the process of “signing on” to an IT resource...”
- In paragraph 7 of the subsection related to Monitoring Certain Information Technology (IT) Controls, the panel on the right side of Figure 1, *Monitoring Tools*, discusses the general nature of “Tools That Identify Changes in Systems.” We suggest you clarify what is meant by the bullets “Communicate” and “Consistency” and how these bullets relate to the topic.