Guidance on Monitoring Internal Control Systems

Dear Professor Rittenberg:

Ernst & Young LLP is pleased to comment on The Committee of Sponsoring Organizations of the Treadway Commission’s (“COSO”) Guidance on Monitoring Internal Control Systems (“Guidance”). We believe the Guidance significantly improves upon the Discussion Document that was exposed for comment in September 2007 and we commend COSO’s efforts to incorporate our earlier comments and suggestions. We believe the important concepts outlined in the Guidance will be of significant aid to organizations wanting to better understand how effective monitoring can help to provide reasonable assurance about the ongoing effectiveness of the system of internal control as a whole. We further believe the application techniques provided in Volume III will aid companies in designing and implementing their monitoring programs.

We offer the following comments and observations that we believe will improve the Guidance.

Overall Comments

Designing and Executing Monitoring Procedures

We support the concepts for designing and executing monitoring procedures described in Volume II, Chapter III. However, we believe several concepts presented in this section require additional clarification or discussion.

Paragraph 46 describes the notion of “key controls” and paragraph 47 suggests that focusing on those controls “helps ensure that the organization devotes monitoring resources where they can provide the most value.” We interpret this sentence as suggesting that a focus on “key controls” provides an efficient strategy for monitoring the system of internal control. However, we also observe that COSO expresses a potentially different view in the third caveat under “Applying the Concepts” on page 24 of the Guidance where it states that the example “is not meant to imply that the non-key controls will not be subject to monitoring. They may be monitored in relation to other risks, or the organization may decide to evaluate them less frequently.” We believe that more clearly indicating COSO’s position as to whether or not management should monitor non-key controls, and how that might be done, would significantly aid organizations in determining an appropriate scope of control monitoring.
Paragraphs 43 and 57 describe how meaningful risks and key controls can operate at multiple levels within the organization. We recommend that the discussion in these paragraphs be clarified to indicate that the concept is a function of differing roles and delegated responsibilities and not a function of relevance to the organization. We believe the store or plant-level controls in the examples are also important to achieving organizational objectives. Responsibility for those controls, and the periodic monitoring of them, has been delegated to lower levels of management in the organization. We do not believe it is appropriate to infer that senior management is not interested in the continued functioning of these controls because responsibility for them has been delegated to others. Absent this suggested clarification, we believe these paragraphs might have the unintended consequence of implying that management should only monitor organization-level controls, or might decide to monitor controls only over those risks that warrant the attention of senior management.

We recommend that the discussion of control risk factors in paragraph 58 also include as a factor the risk associated with the control — the risk that the control might not be effective and, if not effective, will materially affect the achievement of the organization’s objectives. We acknowledge that the factors in the current list (complexity, judgment, manual vs. automated, known control failures) each address aspects of risk associated with the control. However, we believe these factors may not adequately address those controls that management might determine materially affect the organization’s objectives and therefore should be monitored simply due to their importance. We also recommend making this point in the table in paragraph 78. While the table addresses the potential effects of a control failure, it does not illustrate that as the likelihood (or risk) of a control failure increases, management may decide to gather and analyze more information to support their conclusions about control effectiveness. We believe organizations can develop more efficient control monitoring programs when they incorporate consideration of both the likelihood and the potential effects of a control failure in determining the nature, timing and extent of their control monitoring.

**Formality of Monitoring and Level of Documentation**

We recommend that certain concepts discussed in the Guidance regarding the formality of monitoring and level of documentation be clarified.

We believe paragraphs 116-117 and the related “Applying the Concepts” section incorrectly implies too close a link between an organization’s external reporting requirements and audits conducted by the external auditor. A number of organizations currently are required to assert to the effectiveness of their system of internal control over financial reporting without a corresponding audit requirement. We believe the Guidance should indicate that when management is required to assert to the effectiveness of an entity’s system of internal control to third parties, it may conclude that the organization should develop and retain more formal documentation to support making the required assertion. Accordingly, we recommend changing the first sentence of paragraph 117 to more clearly reflect that management of an entity that is required to assert to the effectiveness of the system of internal control may have its own need for more formal documentation. We also recommend changing the example in the second sentence of paragraph 117 so that it illustrates the intended point of the first sentence – external reporting requirements may influence management to develop more formal documentation.
We also recommend clarifying that the nature, timing and extent of management’s monitoring procedures also affect the efficiency of third-party evaluations. The fourth bullet point under “Applying the Concepts” indicates how management might consider making cost-effective modifications to the monitoring procedures it performs to improve the efficiency of third-party evaluations. This is an important and distinct consideration that is not addressed in paragraphs 116-118. While the formality of management’s documentation can affect the efficiency with which external auditors and other third parties conduct their evaluations, it is our experience that cost-effective modifications to the actual monitoring procedures also can have a meaningful effect on the efficiency of the evaluations conducted by these parties.

Monitoring Controls Outsourced to Others

We recommend that certain concepts about monitoring controls outsourced to others be clarified and the discussion expanded to more fully describe the procedures that organizations might employ to monitor such controls.

We agree that organizations should understand and prioritize risks associated with outsourced services and should obtain periodic confirmation that the controls at the service provider operate effectively. A service auditor’s examination report is one source of information about the controls of the service provider that are relevant to the user organization. However, such reports are not always available, or the period covered by such reports might not provide timely information for purposes of management’s ongoing monitoring procedures.

We believe that user organizations frequently also rely on other sources of information to monitor the controls of service providers, such as frequent interaction with the service provider, user group forums, user manuals, system overviews, technical manuals, service contracts, and reports by internal auditors or regulatory authorities. Additionally, some user organizations may elect, or find it necessary, to implement effective internal control over the processing performed by the service provider (e.g., comparison of input to output or reconciliation of service provider processing results to other independent records) and therefore may not need to monitor controls of the service provider, or may monitor them on a less frequent basis. In our experience, very few organizations exercise contractual “right to audit” clauses as a means to monitor controls outsourced to others.

We also observe that this section of the Guidance refers to a service auditor’s examination as an “independent audit performed of the controls that are relevant to the user organization.” Because a service auditor’s examination differs from an audit of financial statements, we recommend that the Guidance use the term “engagement” to highlight the distinction.
Detailed Comments

The following is a summary of our more detailed comments and observations where we believe readers would benefit from further clarification. We have organized our detailed comments to correspond with the applicable discussion questions provided in the request for comment. We have not provided a response to every question.

Volume II – The Guidance

Chapter II. Establishing a Foundation for Monitoring

Question 3: Is the model for monitoring presented in paragraph 19 a complete and accurate outline of the monitoring process?

We believe Figure 3, The Monitoring Process, provides a complete and accurate outline of the monitoring process. However, we recommend that COSO more closely correlate the description of the monitoring steps under (2) Designing and executing monitoring procedures and (3) Assessing and reporting results in paragraph 19 with the corresponding items in Figure 3. For example, there are four bullet points in the second chevron, Design and Execute, in Figure 3; however only the first bullet point, Prioritize risks, easily correlates to a bullet point under (2) Designing and executing monitoring procedures, in paragraph 19.

Chapter III. Designing and Executing Monitoring Procedures

Question 9: The Guidance indicates that effective and efficient monitoring evaluates controls that address "meaningful risks" to an organization’s objectives. Paragraphs 50 – 54 provide guidance regarding assessing risks and how prioritizing risk influences monitoring. The intent is to provide guidance (1) without being prescriptive as to how risk assessment should be done, and (2) without delving so deeply into the risk assessment component that the focus of the Guidance shifts away from monitoring. Do you believe the Guidance properly addresses the role of risk assessment in the context of internal control monitoring?

We agree with the concepts discussed under Understand and Prioritize Risks. However, we believe the last sentence of paragraph 51 might inappropriately convey too casual an attitude toward ongoing assessment of risks. We recommend the Guidance emphasize the importance of a company’s ongoing risk assessment process because the conclusions from the risk assessment influence the nature and scope of monitoring.

We agree with the discussion in paragraph 52 that the assessment of risk importance is based on the significance (or magnitude) and likelihood of a resulting error or misstatement. However, we observe that the “Rationale” on page 22 considers only likelihood when determining how to prioritize the risk that revenue is recognized in the proper amounts. We recommend adding a sentence to the “Rationale” on page 22 to indicate more explicitly that magnitude was also considered. For example, COSO might indicate that a large portion of the organization’s total revenues is derived from resellers to denote that magnitude, in addition to likelihood, was considered.
Question 13: The Guidance states that reliable information is accurate, verifiable, and from an objective source (paragraphs 73-75). Is the concept of reliability, as described in the document, clear, correct, complete, and useful?

While we agree with the concept of reliability as described in the Guidance, we observe a discrepancy in the way the term "objective" is defined. In paragraph 73, reliable information is described as "accurate, verifiable, and comes from an objective source." The definition in the glossary states that objective is a measure of the factors that might influence any person to report inaccurately or incompletely information necessary for evaluators to reach appropriate conclusions. It includes personal integrity, as well as factors that might motivate even a person with perceived high integrity to misrepresent facts, such as having a vested, personal interest in the outcome of the monitoring procedures." The definition of objective in the glossary appears to address objective persons whereas the term objective in paragraph 73 appears to refer to an objective source. We recommend clarifying the use and definition of the term objective in the final Guidance.

Question 18: The "Using Technology for Monitoring" section has been simplified from the September 2007 draft, and a discussion regarding "continuous controls monitoring" has been added (see paragraphs 91-94). Is this section clear, correct, complete, and useful? (Note: Some commenters to the September 2007 discussion document indicated a desire for direction in applying the monitoring guidance to controls over information technology (IT). A comprehensive discussion regarding monitoring IT controls has been included in Volume III.)

We agree with the concept that process management tools are designed to make monitoring more efficient and sustainable by automating certain monitoring activities. However, we do not readily understand how process management tools can be used to assess risk and define or evaluate controls without specific examples. We believe that process management tools may assist management in gathering and organizing information that management uses in its monitoring procedures and communicating the results; however, we do not believe such tools would be used to assess risks and define and evaluate controls.

* * * * *

We would be pleased to discuss our comments with COSO or its staff at your convenience.

Very truly yours,

Ernst & Young LLP