

August 14, 2008

Thank you for the chance to comment on this draft. I have attached both the Public Comment Form, and a separate document with my more detailed page-by-page comments.

Unfortunately, I do not believe this document achieves its intended purposes, and will serve to further confuse the readers' understanding of the COSO framework of internal controls.

The most basic concerns with the documents, and one echoed in my comments, is the tendency of these draft documents to:

1. Depart from the original COSO definitions by continually miss-identifying typical Control Activities as Monitoring efforts.
2. Identify Risk Responses, not a part of internal control per COSO definitions, as components of internal control.
3. Use the term "risk" differently than in the COSO definitions - sometimes as "impacts" and other times as ineffective controls, but almost never consistently with COSO's original definitions.
4. Shift the focus from "organizational objectives" to "objectives of internal control" in defining the COSO categories of objectives.

I would be happy to discuss any questions or comments you have.

Larry Hubbard

U.S. Mobile and Work Phone: +1(301) 529-8118

<mailto:Larry@LHubbard.com>

<http://www.LHubbard.com>

### Overall concerns

- Control Activities are ignored, and often identified as Monitoring.
- Risk responses, as management functions, are often called Control Activities.
- Many examples of risks are ineffective or missing controls, or impacts.
- COSO ERM is ignored
- All of internal control is looked at as about mitigating risks, rather than Risk Assessment being only one part.
- Existing management controls, like ISO, etc. are ignored.

### Exec Summary

Page 1 – It seems odd there is no mention of the COSO ERM document. The same is true for the other monitoring documents. Is ERM now an orphan?

Page 3 – This document refers to the three Internal Control Objectives (of which ICFR is one). Other COSO documents, including COSO IC, referred to those as business objectives. Is there a difference – I think so, and it should be addressed if a change from the original COSO framework is intended.

## Comments on COSO Monitoring Drafts

---

Page 5, #17 – This board-level role really should be linked to or called governance, to match the typical usage of the term governance.

### Guidance Volume

Page 3 – The footnote 6 states “The activity of correcting deficiencies may also be classified in the risk assessment or control activities component.” However in COSO IC and ERM, both responses to risks and correcting deficiencies are Management Activities, not internal controls. I believe this document continually confuses management functions or activities with internal controls, whereas earlier COSO documents were clear on the distinction.

Page 5 – This further confuses business objectives, such as profit making and strategy, from internal control objectives as referred to in these documents. It does this by referring to: “each internal control objective” and then the footnote brings in COSO’s Enterprise Risk Management — Integrated Framework, 2004, which includes strategy as an additional objective. The monitoring concepts discussed in this document can be applied equally to monitoring of “internal control over strategy”.

Page 6 – Item 17 says “This process view of the COSO Framework also shows that internal controls are developed (1) in response to one or more identified risks that affect the achievement of organizational objectives...” In prior COSO documents, responses to risks are management functions not internal controls. Does this monitoring document intend to change the original COSO framework in that manner?

Page 6 – Item 4 states: “Designing and implementing responses to the risks (e.g., internal control). ... 18. Many organizations design and implement monitoring procedures in conjunction with step #4 above.”

In COSO, this is the definition of a Control Activity, not a Monitoring function. This monitoring document continually confuses Control Activities with Monitoring – I think because it does not consider risk responses to be a management function, as did the original COSO framework.

Page 7 – under Item 2 it states “Are prioritized based on the importance of the control to achievement of the objective (i.e., the risk associated with the control’s failure), and ...” This use of the term “risk” is confusing, and would be better referred to as “potential impact”. Uses continually are confused by the term “risk” so this document should clarify, rather than confuse, that issue.

Page 8 – in Item 3 “Facilitate prompt corrective actions where necessary” per the original COSO framework, these corrective actions are part of the management process, not part of internal control. It is not used incorrectly here, but this is a chance to further clarify the distinction.

Page 10 – at the top in referring to the board, other organizational initiatives, such as TQM, Six Sigma, ISO should be mentioned somewhere in the document, and this would be one place to do it. Continually ignoring the existence of those other methods of achieving objectives is damaging to the acceptance of COSO frameworks in businesses.

Pages 14-15 – The items these pages call monitoring are Control Activities in the COSO framework.

Page 16 – This Applying the Concepts example give good examples of Control Activities, not Monitoring.

## Comments on COSO Monitoring Drafts

---

Page 20 – Absolutely disagree with “Regardless, the assessment considers the importance of the risk *without* considering the expected effectiveness of internal control.” This Inherent Risk Analysis, ignoring the real world control already in place, is the single biggest driver of No Value Added work in the SOX/ICFR process. It makes the Risk Assessment process a theoretical exercise, rather than anything valid to the business. Big mistake.

Page 22 – Both these examples in 55 and 56 are Control Activities, not Monitoring. Not clearly distinguishing these two separate components of control makes this a very confusing document, when compared to the COSO definitions of prior years.

Page 25 – Same comment as above, and risk responses are management functions, not internal controls.

Page 29 – Item 67, these KRI’s and KPI’s are not monitoring, they are Information and Communication, in the COSO framework.

Page 30 -32 – Much of this information is already in internal auditing and external auditing standards, but you’ve chosen to use different words to describe the concepts. It will be confusing rather than useful.

Page 47 – this use of Risk significance and likelihood attempts to measure the impact of existing control deficiencies. That is a different use of the word Risk as a forward-looking concept in the Risk Assessment component. This will be very confusing. A better concept to use here would be Maturity Models related to internal controls.

Page 53 – Item 120 states “The ultimate goal of monitoring is met when organizations use the most efficient means possible to gather and evaluate appropriately persuasive information about the effectiveness

of the internal control system in addressing meaningful risks to organizational objectives.”

NO - risks are only one aspect of internal control. All the COSO components, including RA, relate to achieving objectives. A failure or weakness in control component, such as CE, does impact RA, but it has an impact on all objectives, not just one. So, a weak CE is a "risk" to all objectives, not just one.

Glossary-1 – In Board Monitoring, I wish you’d bring in the word governance here.

Glossary-2 – In Control Objective, this is a much different definition than is used for the COSO Internal Control Objectives (O, F, C). You should recognize the differences between entity and activity level controls, as used in the COSO framework.

Glossary-5 – Objective or objectivity. You also need to define the terms Internal Control Objective, and Business Objective here.

Glossary – also need to define the term “Risk”

### Volume III Application Techniques

Page 31 – This is an unwise example, as it confuses the term risk, with impact. “ 9. Overall, management recognizes that effective store inventory management is crucial to the organization’s operations and financial reporting objectives. As a case in point, we will follow one of those risk factors, “Inaccurate/improperly adjusted store inventory balances” (risk factor 2.b. below), through the monitoring process.” Just because someone does it this way does not mean it is a clear application of the COSO concepts. It is not.

## Comments on COSO Monitoring Drafts

---

Page 32 Item 11 – These are all “impacts of not achieving the objective” not risks. The example departs from the original COSO framework in its use of the term risk.

Page 33 Items 12-14 – these are all risk responses, which are management functions, not monitoring. This also ignores the existence of the Control Activities component of control.

Page 35 Item 16 – This sounds like a different meaning of the term Key Control from that in the draft COSO Monitoring documents.

Page 44 Item 29 states “The key for each organization is to implement internal control, including monitoring, that adequately manages or mitigates meaningful risks to organizational objectives in a cost-effective manner.” Internal controls are more than just mitigating risks – that is just the Risk Assessment and Control Activities components. The whole of Internal Control is about achieving objectives, and risks are just part of that.

Page 49 Item 16 – These are not “risks” they are just objectives with “not” in them. All these are ineffective controls. This is a very poor example, and not consistent with prior COSO IC document. The whole example is about failure of controls, not risks to achieving business objectives.

Page 50, Item 18 – I wish this would relate to a component of COSO, not just “controls” without any source.

Page 65 – all these items identified as Monitoring procedures are Control Activities in the COSO framework.

## *COSO Guidance on Monitoring Internal Control Systems* Public Comment Form – Spring 2008

Thank you in advance for providing feedback on COSO's exposure draft, *Guidance on Monitoring Internal Control Systems*. Your candid responses will allow us to gauge its effectiveness and improve the final document, benefiting organizations of all sizes and their stakeholders.

This comment form follows the order of the Guidance. You may also complete it online (which is our preferred method of collecting feedback) through a link posted at <http://www.coso.org/guidance.htm>. Each section contains brief questions regarding the Guidance and also offers respondents an opportunity to provide general feedback unrelated to the questions. If you prefer, you may provide feedback without answering the questions. The demographic information requested in the last section will help us group and analyze the responses.

You may submit this form or other written feedback via email to [COSOMonitoring@gt.com](mailto:COSOMonitoring@gt.com) or fax it to COSO Monitoring at 704.337.2979.

We would like to receive all comments by August 15, 2008. Note that they will be posted to the COSO Web site as submitted, with no redaction of identifying information.

If you have any questions about accessing or responding to the discussion document, please contact Jay Brietz at 704.632.6916.

We know your time is valuable, and we thank you again for your thoughtful completion of this comment form. Your feedback is integral to the success of the final document.

**Larry E. Rittenberg, PhD, CPA, CIA**  
Chairman, COSO

## Questions/Commentary

---

### Volume II – The Guidance

#### Chapter I. Monitoring as a Component of Internal Control Systems

1. Does the Guidance adequately describe the role of internal control monitoring (paragraphs 6–10)?

Somewhat

*Comments:*

While Monitoring is correctly defined per the original COSO definition, the remainder of the document consistently identifies Control Activities as components of Monitoring. Most of the Monitoring examples are clearly Control Activities in the COSO definition. Several specific examples, among many, are: in the chart on page 6, item 18 describes Control Activities in referring to step #4, but calls them Monitoring; on page 16, in Applying the Concepts, these activities by a Supervisor are Control Activities, not Monitoring; page 22, item 55-56, this monitoring of Key Controls are all Control Activities.

2. Additional comments regarding Chapter I.

*Comments:*

Page 5, footnote 10 seems to be the only reference to the COSO ERM document. Other than this, the draft is silent on that publication. It seems odd there is no other mention of the COSO ERM document. The same is true for the other Monitoring draft documents. Is ERM now an orphan?

The COSO framework refers to achieving organizational objectives, but this monitoring document introduces, on page 5 and in footnote 10, the confusing term "internal control objectives", and refers us to the ERM Strategy category of objectives. This new way (internal control objectives) of referring to organizational objectives is very confusing, and is not consistent with the other COSO publications.

#### Chapter II. Establishing a Foundation for Monitoring

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

No

*Comments:*

In #2, use of the term "risk" here is as an impact, whereas in COSO "risks" are potential future events. This, and the many of the examples in Application Techniques volume use the term risk incorrectly - that is, as an impact rather than as a risk event. This will further confuse an already confusing term.

4. Do you agree with the description of the roles of management and the board with respect to monitoring (see paragraphs 23–24)?

Yes

*Comments:*

But, I wish the term Governance could be used to explain the importance of that key term. There are several other opportunities to do this in referring to the role of the board.

5. Do you agree with the description of the characteristics of evaluators (see paragraphs 25-33)?

Yes

*Comments:*

6. Is the discussion about establishing a baseline understanding of internal control effectiveness clear, correct, complete, and useful (see paragraphs 34–36)?

No

*Comments:*

This section tries to apply the Risk Assessment component of COSO (risks due to change) to the Monitoring. That makes it way too confusing. Most of it also describes Control Activities.

Also, this application is too risk focused - what about other components of control - they need monitoring also. Everything is not about "risks", although from this document one gets that idea. This also explains a Control Activity - not Monitoring.

7. Additional comments regarding Chapter II.

*Comments:*

### Chapter III. Designing and Executing Monitoring Procedures

8. Figure 7 on page 18 and paragraphs 42–49 are designed to provide an overview of the core of monitoring — designing and executing monitoring procedures. Do the graphic and related summary paragraphs properly summarize the process of monitoring?

No

*Comments:*

This Figure describes the Risk Assessment and Control Activities of COSO, not Monitoring. The confusion in this whole document between Monitoring and Control Activities is an unfortunate departure from the COSO internal control and ERM documents, and will lead to enormous confusion.

In the same vein, this document spends times talking about risk responses as a part of internal control, and establishing monitoring for those responses. But, in the prior COSO documents, the actual risk responses are not part of internal control, but a management activity. Not recognizing this causes, I think, the confusion of Monitoring and Control Activities.

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?

No

*Comments:*

I believe there are already enough terms related to risk - inherent, residual, control, alpha, beta, impact, probability, likelihood, etc, etc, that coining another term "meaningful" risk is a bad idea. I wish you would not invent new terms, but use existing ones.

Also I absolutely disagree that an inherent risk analysis is the only way to do this. Inherent risk assessment is not possible in practice, only in theory. Asking one to suspend all knowledge of existing controls is inefficient, and leads to management rejecting the importance of the risk assessment process as a theoretical exercise.

10. The Guidance defines the term “key controls” (see paragraphs 46–47 and 55–57). The project team chose to define the term because (1) it is widely used in practice, but is not consistently defined; and (2) the Guidance proposes that, in order to conclude that the internal control system effectively addresses a given risk, organizations may not need to evaluate every control that addresses that risk — thus, the term distinguishes between controls that will be subjected to monitoring procedures and those that will not. Do you believe the concept of “key controls” is properly addressed in the Guidance?

No

*Comments:*

If you are going to define the term, I wish it matched one of the ways Key Controls is "widely used", rather than inventing a new one. This essentially ties Key Controls to only to risks - but most people, and the COSO definitions, would have Key Controls in the other components of control, such as Control Environment and Information & Communication.

11. Information that is evaluated to assess controls effectiveness provides varying levels of support. The Guidance defines “persuasive information” as that which is capable of providing adequate support for a conclusion about the effectiveness of internal control. Persuasive information is further defined as that which is “suitable and sufficient in the circumstances” (see paragraphs 59–60). Do you agree with the general premise of persuasive information as outlined in the Guidance?

Somewhat

*Comments:*

However, many of these concepts are already defined in internal and external auditing standards. I wish you could use existing standards rather than creating new ones, and new terms.

12. The Guidance discusses the difference between direct and indirect information as being one of the primary factors influencing the persuasiveness of information. Feedback from the September public discussion document indicated broad support for this aspect of the Guidance, but also indicated a need to refine and clarify the material. Is the current discussion of direct and indirect information (in paragraphs 64–72 and in the Applying the Concepts section beginning on page 34) clear, correct, complete, and useful?

Somewhat

*Comments:*

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?

Somewhat

*Comments:*

14. Is the concept of timeliness of information (paragraphs 76–77), as described in this document, clear, correct, complete, and useful?

Somewhat

*Comments:*

15. The “Sufficient Information” section (paragraphs 78–79) has been expanded based on feedback from the September public discussion document. Is this expanded material clear, correct, complete, and useful?

Somewhat

*Comments:*

16. Based on feedback from the September discussion document, the section regarding “Ongoing Monitoring and Separate Evaluations” has been simplified. It now more clearly articulates that the primary difference between the two is not how they are performed, but how often and by whom. The Guidance then addresses the factors an organization might consider in deciding between the two processes. Do you believe this section is clear, correct, complete, and useful?

Yes

*Comments:*

17. A paragraph has been added to the document to address the monitoring of controls outsourced to others (paragraph 90). Is this paragraph clear, correct, complete, and useful?

Yes

*Comments:*

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.)

No

*Comments:*

I believe this discussion is related to the Control Activities and Information & Communication components of internal control, not to Monitoring.

19. Additional comments regarding Chapter III.

*Comments:*

The "Channel stuffing" example repeatedly confuses the Control Activities component of control with risk responses (which are a management activity). It does not aid in a proper understanding of the concepts.

## Chapter IV. Assessing and Reporting Results

20. Is the section “Prioritizing and Communicating Results” clear, correct, complete, and useful?

Somewhat

*Comments:*

In the table on Page 47, usage of the term "risk" applied to a known weakness is different than the use of risk in Risk Assessment.

The concept of Maturity Models really needs to be introduced here.

21. Is the section “Reporting Internally” clear, correct, complete, and useful?

Yes

*Comments:*

22. Is the section “Reporting Externally” clear, correct, complete, and useful?

Yes

*Comments:*

23. Additional comments regarding Chapter IV.

*Comments:*

## Chapter V. Scalability of Monitoring

24. Chapter V, “Scalability of Monitoring,” is designed to show how monitoring might differ between organizations based on their size and complexity. It is designed to complement and summarize other references to size and complexity that are spread throughout the document. Is this chapter clear, correct, complete, and useful?

Yes

*Comments:*

## Section VI. Assessing the Effectiveness and Efficiency of Monitoring

25. Is Chapter VI, “Assessing the Effectiveness and Efficiency of Monitoring,” clear, correct, complete, and useful?

No

*Comments:*

NO - not correct. Risks are only one aspect of internal control. All the components, including RA, relate to achieving objectives. A failure or weakness in control component, such as CE, does impact RA, but it has an impact on all objectives, not just one. So, a weak CE is a "risk" to all objectives, not just one.

## Other General Areas/Topics

26. Does the Executive Summary (Volume I) effectively summarize the guidance contained in Volume II?

Somewhat

*Comments:*

27. Apart from your comments above, should anything be added or changed to improve the Guidance, making it more practical to implement? If so, please summarize your recommended additions or changes below.

[Click Here to Select Response](#)

*Comments:*

The COSO component Control Activities are largely ignored, and often identified as Monitoring.

Risk responses, as management functions, are often called Control Activities.

Many examples of risks are ineffective or missing controls, or impacts, rather than potential future events with a possible impact and probability. This departs from past COSO documents.

COSO ERM is ignored

All of internal control is looked at as about mitigating risks, rather than Risk Assessment being only one part of internal control.

Existing management controls, like ISO, TQM, Balanced Scorecards, etc. are ignored in all

these documents.

28. Overall, do you believe the document advances the understanding of what effective monitoring should look like in any given organization?

No

*Comments:*

These documents will provide much additional confusion, as while they state the original COSO IC and ERM frameworks and definitions are still valid, most of the examples are NOT consistent with those frameworks. Much additional confusion will follow.

## Volume III – Application Techniques

### Chapters II–IV. Brief Examples Linked to Volume II Chapters

29. Chapters II–IV of Volume III contain brief examples of how various organizations currently monitor internal control in ways that are consistent with the concepts embodied in Volume II — the Guidance and are organized to correspond with the Guidance. As the introduction to Volume III indicates, the examples are not intended to mandate how monitoring should be performed, but to articulate how the Guidance might be applied. Do the examples achieve that objective? (Note: Please elaborate if you believe certain of the examples should be edited or deleted or if you recommend inclusion of other examples.)

No

*Comments:*

30. The appendices to Volume III relate to the examples discussed in question #29 and show some of the tools the various organizations use for monitoring. Are the appendices helpful without appearing to be prescriptive?

Somewhat

*Comments:*



## Chapter V. Comprehensive Examples

31. Chapter V of Volume III contains comprehensive examples of how two organizations monitor internal control over a given risk area. These examples attempt to demonstrate application of the monitoring process from start to finish, as outlined in the Guidance. Like the earlier examples, those in Chapter V are intended to be descriptive rather than prescriptive. Do these two examples help demonstrate application of the Guidance?

[Click Here to Select Response](#)

*Comments:*

Large Retail Organization's Monitoring of Controls over Store Inventory – This is an unwise example, as it confuses the term risk, with impact. Especially starting on page 32. Just because some company does it this way does not mean it is a clear application of the COSO concepts. This is not.

32. Chapter V of Volume III also contains a discussion of monitoring information technology (IT) controls that address financial reporting-related risks. This discussion was included because (1) many people have requested specific guidance regarding monitoring IT controls related to financial reporting, (2) IT-related risks are pervasive across most organizations, and (3) the ways in which those risks are controlled are fairly consistent across organizations, making the discussion applicable in a broad sense. Without being prescriptive, does the discussion about monitoring IT controls articulate how such monitoring might be performed?

No

*Comments:*

This approach links "Nature of Risks" to Risk Descriptions, and derives controls from those risks. This "risks first" approach is much less effective than a "control objective" approach such as in the COBIT framework. This example will further confuse the assessment of IT controls.

33. Additional comments regarding Volume III.

*Comments:*

---

### Demographic Information

34. Your name

Larry Hubbard

35. Your email address

Larry@LHubbard.com

36. Your position (select the position from which you answered the questions above)

Consultant

37. Country

United States

38. Name of organization (should correspond to position selected in Question 36 above)

Principal

39. Classification of the above-named organization (select one)

Private company/sole proprietorship

40. Annual revenues of the above-named organization

N/A

41. Public float (market cap) of the above-named organization, if a public company

N/A