

To whom it may concern,

Please find attached my comment letter in the standard format WORD file.

Kind regards,
Cees Klumper

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 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:

The Guidance in some places creates the impression that change identification and change management ("CI/CM") should be part of monitoring (in par. 9 and particularly in par. 23 of Volume I and par. 35 of Volume II as well as in several other places).

In the graphic appearing first in par. 22 of Volume I and in par. 35 of Volume II, monitoring is correctly shown as being separate and distinct from CI/CM. CI/CM should indeed be regular process activities with their own controls to oversee them; the combination of the two should be subject to monitoring just like other important process & control activities.

To avoid possible confusion as to how CI/CM 'fits in', I recommend changing some of the wording that now creates the impression that CI/CM should be part of organizations' monitoring activities, rather than process & control, activities, including in the graphic appearing in par. 22 of Volume I and par. 35 of Volume II (see also my response to question 7).

2. Additional comments regarding Chapter I.

Comments:

The importance of the concepts articulated in the Guidance cannot be over-emphasized as particularly larger organizations can benefit greatly from implementing them. Drafting and issuing the Guidance is an important first step but much more will have to be done to get organizations to actually implement it.

After all, the concept of monitoring was already well-described in the original and subsequent COSO publications, but most organizations have yet to put the monitoring concept in place as COSO intends. So making available yet more guidance, no matter how correct and practically-oriented as the Exposure Draft is, will probably not be sufficient; companies will have to adopt it in practice and in my personal experience this is far less likely to happen than one might expect.

Accordingly, I encourage the Committee and especially its constituent organizations to undertake significant promotional efforts to convince organizations to actually put the Monitoring Guidance into practice.

As a thought, it could be worthwhile to form a group of volunteer organizations that share their experiences as they set out to implement the Guidance, facilitated by for example representatives from the COSO taskforce, to enable the fine-tuning of the Guidance or develop Q&A-type materials that can benefit others.

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?

Yes

Comments:

Actually the model referred to in par. 19 is still part of chapter I.

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:

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)?

Somewhat

Comments:

As indicated in my answer to question 1, the discussion in par. 35 about how change identification and change management 'fit in' can be improved.

For example, I would recommend changing the second sentence of par. 35 from:

"With the baseline as a starting point, organizations can design ongoing monitoring and separate evaluations to identify and address changes as they occur"

to something like:

"With the baseline as a starting point, organizations can design processes and procedures to identify and address changes as they occur."

Sub-paragraph 2 of par. 35 then accurately describes how monitoring oversees other procedures' effectiveness in identifying and managing change, for example as part of the Risk Assessment component of internal control.

7. Additional comments regarding Chapter II.

Comments:

The last sentence in paragraph 36 seems out of context ("As a result, change-identification and change-management processes can influence the scope of other monitoring procedures that may be more costly.")

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?

Yes

Comments:

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?

Yes

Comments:

Given the global reach of the COSO framework (for example, in the Netherlands, COSO was the only framework referenced in 2007 annual reports published by listed companies) I would recommend that reference to monetary amounts are done in a 'neutral' fashion, i.e. not to "\$" or to other specific countries' currencies. For example, in par. 54 I suggest leaving out the "\$" sign in from of "amounts" in the fourth line of the first bullet. Likewise, on page 34, fourth bullet, I would suggest changing "dollars" to "monetary amounts".

On page 21 I would suggest striking the phrase "what can go wrong" in the second sentence under "applying the concepts"; it is redundant given the second part of the sentence:

"Management can begin the analysis by reviewing its financial statements and asking what can go wrong or what might reasonably prevent the organization from achieving its financial reporting objectives in a given area."

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?

Yes

Comments:

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?

Yes

Comments:

For the sake of clarity, I recommend adding a table/graphic at the start of this section that depicts the various different types of information discussed that the reader can refer to, for example as follows:

Persuasive =
 Suitable + Sufficient
 (= relevant + reliable + timely)

I also recommend changing the first sentence of par. 59 from:

"The 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."

to:

"The persuasiveness of information refers to the degree to which the information used in monitoring can adequately support a conclusion regarding the effectiveness of internal control."

I did not find Figure 8 on page 28 to be particularly useful and recommend deleting it.

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?

Yes

Comments:

Personally I found this part (about the different kinds of information that can be used in monitoring) of the Guidance to be more theoretical than probably necessary; the risk in that is that it may detract from the overall document and discourage practitioners from actually applying the Guidance in practice - especially those who, like myself, subscribe to the 'less is more' concept.

In the table on page 72, I recommend adding a row that addresses the factor "recent experience with control performance" - where there have been relatively few instances of

control failure, it may be appropriate to use less direct and more indirect information.

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?

Yes

Comments:

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

Yes

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?

Yes

Comments:

I would recommend adding, as factors to consider in the table on page 32, "length of time since last more in-depth evaluation" and "recent experience with control performance"

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:

This is going to be one of the areas that will be the most difficult for organizations to grasp because, in practice, I have found that, in many organizations, there is a significant amount of ongoing monitoring that is performed by functions that also perform separate evaluation-type activities. Consider for example an internal control department that, in essence, performs a monthly routine verification of the performance of certain controls in lieu of management or other individuals performing that task - in many cases because it is considered to be more efficient that way. At the same time, that same internal control department can perform certain sample-based testing activities that are not routine and would fit the definition of separate evaluations. Another example is that of an operational risk function within a financial services institution that regularly performs ongoing monitoring, as well as separate evaluation-type activities. So although I believe the Guidance is clear, I expect that, in practice, organizations will have trouble making the distinction.

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.)

Yes

Comments:

19. Additional comments regarding Chapter III.

Comments:

On page 17, I recommend changing par. 40 to:

"In order to implement monitoring that provides the necessary level of support, organizations must determine, among other things:

- What controls to monitor,
- What monitoring procedures to employ,
- How often to employ them,
- Who should perform them,
- A protocol for communicating findings from monitoring
- Documentation guidelines"

On page 25, I recommend replacing the word "test" by "monitoring procedures" as follows (the word "test" is often associated with separate evaluation-type monitoring which is not a desirable association in this context):

Change text under control example 1 from:

"Therefore, this control is not selected as a key control, thus reducing the potential to develop unnecessary redundant tests — one of the standardized contract control and another of the standardized contract modification approval control."

to:

"Therefore, this control is not selected as a key control, thus reducing the potential to develop unnecessary redundant monitoring procedures — one of the standardized contract control and another of the standardized contract modification approval control."

There are other similar references to "tests" that should be replaced by "monitoring procedures" throughout the remainder of the Guidance, for example in par. 66 and footnote 20 there are references to "direct testing"; in my opinion this term should be avoided (also I

do not believe it is defined in the Guidance anywhere) because it is commonly associated with procedures performed by external or internal auditors, although in this context it is intended to also describe possible ongoing monitoring procedures.

In some of the examples provided, some controls are presented as 'dual-purpose' (i.e. being both a control as well as a monitoring activity). Given that the distinction between the two is at best 'blurry' with most people to begin with, I would recommend adding some explanatory language the first time a 'dual-purpose' control is presented.

Chapter IV. Assessing and Reporting Results

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

Yes

Comments:

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?

Yes

Comments:

Other General Areas/Topics

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

Yes

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.

Yes

Comments:

In line with my response to question 2, I recommend that the Committee formulate a plan of action as to how it will encourage and facilitate adoption of the Guidance by organizations beyond providing the Guidance.

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

Yes

Comments:

I believe that the Guidance will be a landmark in the thinking and practice of internal control. But it will take many years before it will have made the impact that it should.

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.)

Yes

Comments:

I strongly recommend adding a few examples on the internal reporting of the results of ongoing monitoring. In the current draft, there are really only examples of reporting on the results of separate evaluation-type activities. Example 40 does not add much value in my opinion.

In line with my earlier comment, several of the examples use the word "test" to describe ongoing monitoring activities. I would strongly recommend changing this wording to terms more appropriate in the context of ongoing monitoring, such as "review" to be internally consistent. For example, on page 13, halfway down the page, there are references to "audit program" and "test" that should be changed. Similarly on page 15, toward the bottom, there is a reference to a "test" of controls over data entry that should be changed to, for example, "review". On page 17, in the second paragraph, there is a reference to "audits" that should be changed, for example to "reviews" and on the same page, just below the middle in the "labor" paragraph, there is a reference to "direct testing" that should be changed, for example to "reviews". Same comment on page 18, second paragraph and page 22, example 31, I would recommend either striking the words "independent testing" or replacing them with "separate evaluations". In example 35, I suggest replacing "test" with "review". There are several references to "testing" in appendix A-2, paragraph 2 that should be changed. Finally, there are several references to "test plans" and "test" / "testing" in the appendices that I recommend changing.

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?

Yes

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?

Yes

Comments:

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?

Yes

Comments:

33. Additional comments regarding Volume III.

Comments:

Appendix A-2, par 1, second line: "framework for internal controls over financial reporting" should probably be "framework for internal control over financial reporting".
Appendix A-4, second line: "effect" should probably be "affect"

Demographic Information

34. Your name

Cees Klumper RA MBA CIA

35. Your email address

cees@klumper.demon.nl

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

Other (please describe)

A private individual with a keen interest and significant experience in this very topic!

37. Country

The Netherlands

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

n/a

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

Other (please describe)

private individual

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