



3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA

Telephone: 847.253.1545
Facsimile: 847.253.1443

Web Sites: www.isaca.org and www.itgi.org

13 August 2008

COSO Board of Directors

Via e-mail COSONitoring@gt.com

Also online at <http://www.coso.org/guidance.htm>

RE: *Internal Control—Integrated Framework: Guidance on Monitoring Internal Control Systems* Volumes I Executive Summary, II Guidance and III Application Techniques Exposure Drafts

Dear COSO Board of Directors:

Congratulations on the issuance of the exposure draft *Internal Control—Integrated Framework: Guidance on Monitoring Internal Control Systems* (“the draft”). We very much appreciate the opportunity to provide comments on it. These comments are offered on behalf of ISACA and the IT Governance Institute (ITGI), in my capacity as chair of the Professional Issues Working Group and former international president of both organizations.

With more than 86,000 constituents in more than 160 countries, ISACA (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor (CISA) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager (CISM) designation, earned by more than 9,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT (CGEIT) designation.

The IT Governance Institute® (ITGI™) (www.itgi.org) is a nonprofit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the nonprofit membership association ISACA in 1998 to help ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly managed, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfill their IT governance responsibilities and help IT professionals deliver value-adding services.

As the worldwide leading independent thought leaders on IT controls, we are eager to assist COSO in accomplishing its mission. Please feel free to call on our organizations if we can be of assistance in any way on further deliberations, task forces, commissions or committees.

General Comments

As a whole, we support the COSO board's ("the board") goals for the project and the resulting draft, which we believe accomplishes the board's high-level objectives for most businesses. The document is a clear and well-thought-out contribution of key concepts and the overall theory on monitoring, useful to the broadest possible audience. It presents some difficult concepts in a useful manner.

Information technology plays a key role in most internal control systems; however, there is very little discussion of monitoring IT controls in volumes I and II. We recommend that additional guidance on monitoring of IT controls and the role of IT governance be included.

We have included our specific comments in attachment A and a copy of our responses to the COSO online questionnaire in attachment B at the end of this letter.

* * * * *

Again, we appreciate the opportunity to comment on the draft of the COSO guidance on monitoring internal control systems. Thank you for considering our views. We would be happy to discuss them with you in further detail.

Respectfully submitted,



Everett C. Johnson, CPA
Chair, Professional Issues Working Group
Past International President, 2005-2007
ISACA (www.isaca.org)
IT Governance Institute (www.itgi.org)

Attachment A—Comments in Page Order**Volume I**

Page 4, paragraph 13—It would be helpful if the monitoring process diagram included a step titled “taking corrective action,” with perhaps a footnote that corrective action is normally not part of the monitoring process. The model appears incomplete without a “corrective-action step.” This recommendation also applies to volume II, pages 7-8, paragraphs 18 and 19.

Page 8, paragraph 28—The term “important controls” is introduced here and is sometimes used interchangeably with “key controls” throughout all three volumes. We recommend only one of these terms be used and that it be used consistently. The term “key controls” is also used in the glossary.

Page 14, paragraph 57—We recommend that the last sentence of this paragraph be changed to read as follows: “An organization may use a prepackaged information system for one of its business processes, which can reduce certain IT-related risks (such as the risk of incorrect programming), but that same organization might also use a complex internally developed software system for another business process, which, unless well controlled, can increase IT-related risks.” Please see also the comment below on volume II, page 52, paragraph 114 for additional information.

Page 14, section IV—We suggest adding an overview section for volume II similar to the one at paragraph 60 for volume III.

Page 15, paragraph 62, subparagraph 10—We suggest starting the sentence with “Computerized monitoring tools have undergone...” for improved clarity.

Volume II

Page 9, paragraph 24—Unless there is a clear example of when a board is not ultimately responsible for determining whether management has implemented effective internal control, we suggest deleting the phrase “In most cases” at the start of this paragraph.

Page 15, paragraph 36—We suggest adding the following two sentences just before the last sentence: “This approach may be particularly effective and efficient in highly computerized environments, because many automated systems can provide a listing of all changes to system applications and programs, to configuration settings, and to the authorization of persons who can perform important functions. This change information can be used by automated monitoring tools and can serve as a source of monitoring information for manual review.”

Page 19, paragraph 46, first bullet—We suggest revising to read “...affect the achievement of the organization’s objectives if their failure would not be reasonably detected in a timely manner by other controls, and/or...” for improved clarity and consistency with volume I, paragraph 7.

Page 33, table item “Automated Controls”—We suggest revising the first sentence to read “Automated controls generally operate consistently when they exist in a well-controlled IT environment.”

Page 41, paragraph 92—We suggest adding the following sentence as part of the normal paragraph at the end of the bullet list: “The reports provided by these tools need to be reviewed by knowledgeable individuals on a timely basis and exceptions reported to those responsible for taking corrective action.”

Page 46, paragraph 98—It is not clear what is meant in the last sentence by “appropriately objective personnel” and its use here does not appear consistent with the glossary definition. We believe wording such as “management personnel with an appropriate level of authority” might be more appropriate.

Page 52, paragraph 114—We have a number of concerns regarding this paragraph:

- The paragraph is about scalability, but introduces the concepts of prepackaged software and accounting for derivative contracts and attempts to characterize the risks related to them.
- The paragraph uses the terms “IT risks” and “accounting risks,” which are not defined anywhere. These terms are also used elsewhere in the three volumes, but not always consistently. We would prefer the terms “IT-related risk” and “financial reporting risk” be used consistently and defined in the glossary.
- The paragraph implies that the use of prepackaged software reduces all “IT risk,” while, in fact, it may reduce only the risk of incorrect programming and then only if programming changes are not allowed and software updates are properly applied on a timely basis.

We suggest the following:

- Add a new paragraph before paragraph 114: “An organization may use complex IT systems that are subject to IT-related risks such as: inappropriate access, program integrity, data integrity and information processing (as discussed further in volume III, page 59). IT processing may be centralized or decentralized, which can affect scalability. In a centralized IT processing environment, certain IT control monitoring activities (such as those over system changes or access controls) may be monitored once, thereby providing monitoring leverage over a number of other controls that otherwise would need to be monitored separately.”
- Change the last sentence of paragraph 114 to read as follows: “An organization may use a prepackaged information system for one of its business processes, which can reduce certain IT-related risks (such as the risk of incorrect programming), but that same organization might also use a complex internally developed software system for another business process, which, unless well controlled, can increase IT-related risks.” The sentence about complex derivative contracts should be deleted.

Glossary—We suggest revising the definitions of “accuracy” and “compensating controls” so that they are complete sentences, as are the rest of the definitions. We also suggest adding definitions for “IT-related risk” and, if the term is used, “financial reporting risk.”

Volume III

Page 4, example 3—We believe this is an inappropriate example in its present form. An internal audit function should not be implementing a rewards system as that can create a less-than-objective situation for the internal auditors. We recommend that the example be changed to

remove any implications that internal audit is affecting the compensation or other rewards of employees with control responsibilities (e.g., the indicated function could be performed by a compliance group or risk management group, with internal audit playing a more traditional role) or that the example be deleted.

Page 60, paragraph 3, first bullet at top of page—We suggest ending the sentence after “...conceal illegal activity is a greater risk.”

Page 60, Program Integrity, first bullet under “Example Factors”—In the first sentence, we suggest changing “typically carry” to “may carry.” In the next sentence, we suggest using “On the other hand” instead of “However.”

Page 61, paragraph 4—The CFO example in the last paragraph is an example of a compensating control and it provides only indirect information, if any, about the operation of IT controls. A better example of manual monitoring of IT controls might be along the following lines: “For example, in a small organization, the Chief Financial Officer (CFO) may review the monthly reconciliations of the input and output balancing controls that ensure completeness of processing for the significant financial processing applications. This monitoring of the reconciliation process enables the CFO to easily identify whether the reconciliations have been performed by the responsible control party, and to review the disposition of any differences.”

Page 61, paragraph 5—We suggest that the end of the first sentence be modified to read “... one or more of the broad risks *related to financial reporting* defined earlier.”

Page 69, paragraph 13—The example of the POS system describes control procedures to ensure the accuracy and completeness of store data; however, the use of these tools and process for monitoring is unclear. This should be clarified, perhaps with the addition of a paragraph similar to that on page 70, paragraph 15.

Page 70, paragraph 17—This paragraph also should be clarified to indicate how the problem management process can be used for monitoring.

Page 71, paragraph 18—We suggest changing “information technology risks” to “IT-related risks.” See the previous comment on volume II, page 52, paragraph 114.

Page 71, paragraph 19—We suggest deleting the CFO example for the reasons discussed above (see page 61, paragraph 4).

Appendix B-8, Section G—We suggest adding a question after G.16 as follows: “Have there been any changes to systems and processes (including IT systems and processes) that could adversely affect internal control or that may require new controls or changes to existing controls?” Alternatively, a separate representation from the CIO, focused on IT systems and controls, compliance issues, etc., might be included.

Attachment B—Responses to COSO Online Questionnaire**VOLUME II - THE GUIDANCE****Chapter I. Monitoring as a Component of Internal Control Systems (pages 1-7)**

1. Does the Guidance adequately describe the role of internal control monitoring (paragraphs 6-10)?
 Yes No
2. Additional comments regarding Chapter I.

Chapter II. Establishing a Foundation for Monitoring (pages 8-16)

3. Is the model for monitoring presented in paragraph 19 a complete and accurate outline of the monitoring process?
 Yes No

Comments: Please see our comments in Attachment A.

4. Do you agree with the description of the roles of management and the board with respect to monitoring (see paragraphs 23-24)?
 Yes No

Comments: Please see our comments in Attachment A.

5. Do you agree with the description of the characteristics of evaluators (see paragraphs 25-33)?
 Yes No Somewhat

Comments:

6. Is the discussion about establishing a baseline understanding of internal control effectiveness clear, correct, complete, and useful (see paragraphs 34-36)?
 Yes No Somewhat

Comments: Please see our comments in Attachment A.

7. Additional comments regarding Chapter II. Please see our comments in Attachment A.

Chapter III. Designing and Executing Monitoring Procedures (pages 17-44)

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 No Somewhat

Comments: Please see our comments in Attachment A.

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 No Somewhat

Comments:

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
_X_Yes _No _Somewhat

Comments: Please see our comments in Attachment A.

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?
_X_Yes _No _Somewhat

Comments:

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?
_X_Yes _No _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?
_X_Yes _No _Somewhat

Comments:

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

_X_Yes ___No Somewhat

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?

_X_Yes ___No Somewhat

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.)

_X_Yes ___No Somewhat

Comments: Please see our comments in Attachment A.

19. Additional comments regarding Chapter III.

Please see our comments in Attachment A.

Chapter IV. Assessing and Reporting Results (45-49)

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

_X_Yes ___No Somewhat

Comments:

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

_X_Yes ___No Somewhat

Comments:

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

_X_Yes ___No Somewhat

Comments:

23. Additional comments regarding Chapter IV. Please see our comments in Attachment A.

Chapter V (pages 50-52)

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 ___No _X_Somewhat

Comments: Please see our comments in Attachment A.

Chapter VI (pages 53-54)

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

Yes No Somewhat

Comments:

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

Yes No 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 suggested additions or changes below.

Yes No

Comments: Please see our comments in Attachment A.

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

Yes No Somewhat

Comments:

VOLUME III - APPLICATION TECHNIQUES

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 No Somewhat

Comments: Please see our comments in Attachment A.

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 No Somewhat

Comments: Please see our comments in Attachment A.

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 No Somewhat

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 No Somewhat

Comments:

Please see our comments in Attachment A.

33. Additional comments regarding Volume III.

Demographic Information

34. Your name: Everett C. Johnson, CPA
35. Your e-mail address: research@isaca.org
36. Your position: Chair, Professional Issues Working Group, and Past International President, 2005-2007
37. Country: International Association
38. Name of organization (should correspond to position selected in Question 36):
ISACA (www.isaca.org) and IT Governance Institute (www.itgi.org)
39. Classification of the above-named organization: Professional Association
40. Annual revenues of the above-named organization:
 Greater than \$10 billion
 \$5B to \$10 B
 \$1B to \$5B
 \$500M to \$1 Billion
 \$100M to \$500M
 Less than \$100 million
41. Public float of the above-named organization, if a public company (not applicable)
 Large accelerated filer
 Accelerated filer
 Non-accelerated filer