



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

31 October 2007

COSO Board of Directors
In care of Dr. Larry E. Rittenberg
School of Business, University of Wisconsin-Madison
4133D Grainger Hall
975 University Avenue
Madison, WI 53706

RE: *Internal Control—Integrated Framework: Guidance on Monitoring Internal Control Systems* Discussion Document

Dear COSO Board of Directors:

Congratulations on the issuance of the discussion document, *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.

ISACA is an international professional, technical and educational organization dedicated to being a recognized global leader in IT governance, security, control and assurance. With 70,000 members in more than 140 countries, ISACA is uniquely positioned to fulfill the role of a central, harmonizing source of IT control practice standards the world over. Its strategic alliances with other organizations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners.

ITGI strives to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise’s mission and goals. Its goals are to raise awareness and understanding among, and provide guidance and tools to, boards of directors, executive management and chief information officers (CIOs). The ultimate goal is to ensure that IT meets and exceeds expectations, and its risks are mitigated.

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 itself, 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 meaningful manner. However, the document should include more detailed guidance and examples to be a useful tool for management. We understand this is COSO's intent.

***Recommendation:** Add examples and more detailed guidance to make this document as useful as possible for management.*

Primary Comments

Our primary comments focus on the following areas:

- Emphasis on the use of “indirect information” for monitoring
- Consistency of control performance
- Lack of material on IT general controls and IT governance
- Incorporation of the effects of regulatory examinations into the monitoring process

In addition, we have included additional comments in attachment A and a copy of our responses to the COSO online questionnaire in attachment B at the end of this letter.

Emphasis on the Use of “Indirect Information” for Monitoring

We have some concern about the degree of emphasis on the use of “indirect information” for monitoring. We believe indirect information provides no evidence about the continuing operation of internal control effectiveness. Notwithstanding the caveats that have been provided, we believe the inclusion of indirect information may result in inappropriate or excessive reliance on such information for monitoring activities.

***Recommendation:** Provide additional guidance—a few sentences to set the tone—limiting the use of indirect information to avoid inappropriate or excessive reliance on such information for monitoring activities.*

Consistency of Control Performance

Consistency of control performance is an important characteristic that can play a critical role in an approach to monitoring; however, it currently receives only a passing reference under “Automated Controls” in the table on page 17.

***Recommendation:** Insert a paragraph on consistency of performance as a characteristic of controls. For instance:*

- *Controls procedures performed by an IT system generally are performed with a very high degree of consistency when the relevant general computer controls are effective. This reduces the extent of activity required for effective monitoring of such IT-based controls.*
- *Many companies have highly standardized control procedures that are consistent across multiple locations. With a strong control environment, such controls are likely to be performed with a high degree of consistency. This can also reduce the extent of activity required for effective monitoring of these types of controls. In addition, where there are many such locations, the risk resulting from a control failure at any one location is likely to be minimal and the likelihood of failures at multiple locations is often very low.*

- *Considering consistency of performance can result in a particularly effective and efficient approach in using the “baselining process” described at the bottom of page 8, particularly in an IT-based environment.*

Lack of Material on IT General Controls and IT Governance

IT general controls play a major role in ensuring that IT systems perform consistently and as intended. IT general controls also contribute to the reliability of information used for control monitoring. As such, IT general controls are a key factor to be considered in monitoring. In addition, an effective approach to IT governance can help provide a strong control environment, an effective risk management program, and appropriate involvement of various parts of the enterprise with IT, thereby contributing to effective monitoring. Comments on general controls should be linked to what is said about the importance of a framework for IT general controls. Monitoring ensures they are working properly.

***Recommendation:** Refine and reincorporate into the September draft the IT general controls and IT governance material on page 19 of the June draft.*

Incorporation of the Effects of Regulatory Examinations Into the Monitoring Process

The document should clarify how the effects of regulatory examinations can be incorporated into the monitoring process.

***Recommendation:** Add a discussion and/or example to clarify how the effects of regulatory examinations can be incorporated into the monitoring process.*

Add an example.

A “clean bill of health” from a regulator/government agency for a bank can be considered and relied upon as a separate evaluation of those controls, provided the scope of the examination is understood and sufficient for this purpose.

* * * * *

Again, we appreciate the opportunity to comment on the discussion document 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—Secondary Comments in Page Order

Page i. While the executive summary is reasonable, it is rather long and we suggest the title could be changed to Executive Focus to more appropriately convey the content.

Page 24. Add to the list of bullets at the top of the page content about tools to monitor access controls and other general controls: For example, a bullet could be added along the following lines:

- IT general controls—Monitoring to ensure that persons with access to key resources remain appropriate, inappropriate access attempts and system changes are reported, and operating and other exceptions are followed up.

Page 24. At the end of the bullet points in the section on Control monitoring tools, add a paragraph on continuous control monitoring and state the benefits (e.g., high effectiveness, low cost). Also, add a paragraph on continuous auditing to clarify the difference between continuous monitoring and continuous auditing, such as:

Continuous monitoring is a management/assurance function implemented by management for compliance and process control, and continuous auditing is a compliance function exercised by an internal or external auditor. Both use a variety of automation tools and formalized business rules, either for auditing or monitoring. The tools can be the same, but the functions are different.

Page 27. We disagree with the last sentence under External Assertions. We believe the information needed to support internal conclusions and external assertions would be the same. We believe the current language may lead readers to believe the information used for internal conclusions could be different from that used for external assertions.

Page 29. The last paragraph on page, which refers to “prepackaged information systems” reducing “IT risk,” should be clarified to indicate the types of controls that are required over such systems and what is meant by “IT risk.” A poorly configured and uncontrolled “prepackaged information system” actually may increase risk. In addition, the paragraph should clarify what is meant by “accounting risk.”

Page 30. Add a middle bullet:

- Formal self-assessments with periodic representations to senior management.

Attachment B—Responses to COSO Online Questionnaire**Section I. Monitoring as a Component of Internal Control Systems**

1. This document says that effective monitoring should be designed to identify and correct weaknesses in internal control *before* those weaknesses can materially impact the organization's objectives. Do you believe the document adequately and properly addresses the concept that, although effective monitoring cannot be expected to identify and correct all internal control weaknesses before they occur, it should be expected to identify and correct them before they lead to material problems?

Yes No Somewhat

Comments: However, we believe this sets a very high bar for effective monitoring.

2. Is the difference between monitoring activities and control activities clear, correct, complete, and useful?

Yes No Somewhat

3. Additional comments regarding Section I.

Comments: Refine and reincorporate into the September draft the IT governance material on page 19 of the June draft.

Section II. Fundamentals of Monitoring

4. This document suggests that effective and efficient monitoring is achieved through:
(1) establishing an effective control environment for monitoring,
(2) prioritizing monitoring procedures based on control importance, and
(3) proper communication and follow-up.

Do you agree with that concept?

Yes No Somewhat

Comments: None

5. The four-point monitoring structure on pages 8 and 9 and in Figure 4 is intended to show how an organization might be able to monitor both efficiently and effectively by focusing on areas of change from a baseline of known effective controls. Is this concept clear, correct, complete, and useful?

Yes No Somewhat

Comments: Emphasis should be made that this approach is particularly effective for well-controlled IT systems.

6. This document suggests that the primary roles of the board/audit committee related to monitoring internal control are to (1) verify that senior management has implemented an

effective monitoring program, and (2) monitor those controls that members of senior management perform and cannot objectively monitor themselves. Is this description of the role of the board/audit committee in monitoring clear, correct, complete, and useful?

Yes No Somewhat

Comments: None

7. Additional comments regarding Section II.

Comments: None

Section III. Nature of Information Used in Monitoring

8. The discussion document uses the term “persuasive information” rather than “evidence” or “persuasive evidence” to describe that which provides evaluators the support they need to form conclusions about control effectiveness. The project team chose the word “information” because the word “evidence” is often perceived to be auditor-centric language. Does the term “persuasive information” adequately convey the intended concept? If not, please suggest another term.

Yes No Somewhat

Comments: None

9. This document suggests that reasonable conclusions about the effectiveness of internal control should be supported by “persuasive information.” It defines persuasive information as that which is *suitable* (referring to the quality of information) and *sufficient* (referring to the quantity of information). Specific questions about suitability and sufficiency follow in questions 10-14 below, but, at a high level, do you agree with this concept?

Yes No Somewhat

Comments: None

10. This document states that suitable information is relevant, reliable, and timely. Information that does not adequately demonstrate all three elements may be suitable to a degree, but alone it cannot support reasonable conclusions regarding continued control effectiveness. Do you agree?

Yes No Somewhat

Comments: None

11. Are the distinctions between direct and indirect information helpful in identifying information that is more versus less relevant?

Yes No Somewhat

Comments: (See accompanying letter.)

12. This document states that reliable information is accurate, verifiable, and from an objective source. Is the concept of reliability, as described in the document, clear, correct, complete, and useful?

Yes No Somewhat

Comments: None

13. Is the concept of timeliness of information, as described in this document, clear, correct, complete, and useful?

Yes No Somewhat

Comments: None

14. This document suggests that companies need to gather *enough* suitable information in order for it to be persuasive. Is the sub-section, "Information Sufficiency," presented on pages 16 and 17, helpful in determining how much suitable information must be gathered in various circumstances to support reasonable conclusions about internal control?

Yes No Somewhat

Comments: None

15. Additional comments regarding Section III.

Comments: None

Section IV. Designing Effective Monitoring (page 18)

16. Is the sub-section, "Prioritizing and Designing Monitoring Procedures"—including the descriptions of the nature of operations, the purpose of monitoring, and the relative importance of controls—clear, correct, complete, and useful?

Yes No Somewhat

Comments: None

17. Are the sub-sections, "Ongoing Monitoring Using Direct Information," "Ongoing Monitoring Using Indirect Information," and "Separate Evaluations Using Direct or Indirect Information," clear, correct, complete, and useful?

Yes No Somewhat

Comments: See comments in accompanying letter.

18. This document states that monitoring using indirect information does not demonstrate explicitly to the evaluator that underlying controls are operating effectively. For example, a supervisor's review of inventory variances does not demonstrate explicitly to him or her that controls over inventory are effective. Do you agree with that concept?

Yes No Somewhat

Comments: See comments in accompanying letter.

19. Is the discussion of capabilities and position of evaluators clear, correct, complete, and useful?

Yes No Somewhat

Comments: None

20. In the sub-section, "Using Technology for Effective Monitoring," the document suggests that technology plays two roles in effective monitoring: control monitoring and process management. The document describes technology tools that can be used to monitor other controls and tools that can assist in the overall management of the monitoring process. Is this section clear, correct, complete, and useful?

Yes No Somewhat

Comments: On page 24, consider adding to the list of bullets at the top of the page content about tools to monitor access controls and other general controls (see accompanying letter).

21. Does the sub-section, "Deciding When and How Often to Monitor," effectively describe how organizations might vary the frequency of their monitoring procedures based on risk?

Yes No Somewhat

Comments: None

22. Additional comments regarding Section IV.

Comments: Add a paragraph on continuous control monitoring tools at end of the bullet points (see accompanying letter).

Section V. Communicating and Addressing the Results of Monitoring Page 25

23. The sub-section, "Ranking Issues and Reporting Internally," describes how organizations might determine what and to whom to communicate the results of monitoring. Does this description provide a better understanding of how to apply Principle 20 from COSO's 2006 Guidance?

Yes No Somewhat

Comments: None

24. Is the section on reporting to external parties clear, correct, complete, and useful?

Yes No Somewhat

Comments: We disagree with the last sentence under External Assertions. We believe the information needed to support internal conclusions and external assertions would be the

same. We believe the current language may lead readers to believe the information used for internal conclusions could be different from that used for external assertions.

25. Additional comments regarding Section V.

Comments: None

Section VI. Scalability of Monitoring

26. The scalability section is designed to show how monitoring might differ between organizations based on their size and complexity. Is this section clear, correct, complete, and useful?

Yes No Somewhat

Comments: On page 29, the last paragraph on page refers to “prepackaged information systems” reducing “IT risk.” It should be clarified to indicate the types of controls that are required over such systems and what is meant by “IT risk.” A poorly configured and uncontrolled “prepackaged information system” actually may increase risk. In addition, the paragraph should clarify what is meant by “accounting risk.”

Other General Areas/Topics

27. Does the executive summary bring into focus the concepts of effective and efficient monitoring?

Yes No Somewhat

Comments: While the executive summary is reasonable in the concepts it addresses, it is rather long. We suggest the title could be changed to Executive Focus to more appropriately convey the content.

28. Apart from your comments above, is there anything that should be added or changed to improve the document, making it more practical to implement?

Additional comments:

- On page 30, add a middle bullet: “Formal self-assessments with periodic representations to senior management.”
- Consider inserting a paragraph on consistency of performance as a characteristic of controls (see accompanying letter).

29. This guidance was developed with the expectation that it would be applicable to monitoring internal control related to all objectives (i.e., objectives related to operations, financial reporting, compliance with laws and regulations, and organizational strategy). However, it was also developed with the expectation that its most-frequent initial application would be related to internal control over financial reporting, particularly by those companies subject to Section 404 of the U.S. Sarbanes-Oxley Act of 2002. Both the U.S. Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) have

published guidance and/or standards related to internal control over financial reporting. Do you believe this document is consistent with the SEC and PCAOB guidance/standards? If not, please identify the conflicts.

Yes No Don't know

Comments: None

30. This discussion document is intended to complement, not to change, the underlying concepts in the original 1992 COSO Framework and in COSO's 2006 Guidance. Do you believe this discussion document is consistent with those documents? If not, please comment on any inconsistencies you have noted.

Yes No Somewhat

Comments: Certain material in the COSO ERM publication might be useful to include or reference.

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

Substantially Moderately Minimally Negatively (more confusing)

Moderately, because more detailed information and examples are needed to implement the guidance. We look forward to the additional implementation guidance to be issued by COSO.

32. If you have either implemented or seen examples of internal control monitoring that you believe represent best practices, please describe them below.

Comments: We would be happy to assist COSO in obtaining such material from our members.