



GAO

Accountability * Integrity * Reliability

Comptroller General
of the United States

United States Government Accountability Office
Washington, DC 20548

November 2, 2007

Dr. Larry E. Rittenberg, Chair
The Committee of Sponsoring Organizations
of the Treadway Commission
University of Wisconsin, School of Business
975 University Avenue
Madison, Wisconsin 53706-1323

Subject: Discussion Document on *COSO Internal Control Integrated Framework – Guidance on Monitoring Internal Control Systems*

This letter provides the U.S. Government Accountability Office's (GAO) comments on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Discussion Document, *COSO Internal Control Integrated Framework – Guidance on Monitoring Internal Control Systems*.

GAO supports the COSO Integrated Framework and COSO's efforts to increase users' understanding of the concepts and applications. We agree with COSO on the importance of properly designed and functioning monitoring processes and procedures and applaud the efforts to increase understanding of effective monitoring, thereby helping organizations improve the efficiency and effectiveness of internal control. Overall, GAO believes the concepts and descriptions in the draft guidance are very helpful in illustrating how monitoring can be made more effective.

We support the risk-based approach to monitoring presented in the discussion document. At the same time, we are concerned that the approach requires a great deal of evaluator judgment without providing guidance for a minimum frequency for monitoring procedures. This, together with (1) the focus on monitoring changes in internal control rather than taking a holistic approach by focusing on control effectiveness, and (2) the extensive discussion on using indirect information to support control assessments, could lead users to perform insufficient monitoring, consequently resulting in erroneous conclusions about control effectiveness.

In addition, the monitoring approach outlined in the proposed guidance starts with establishing a control baseline and then focuses subsequent monitoring on changes from the baseline. To the extent that the organization determines that risks and controls have not changed, it may reduce the frequency of its monitoring procedures. However, this approach may not identify all changes and provides limited information about controls whose effectiveness may have deteriorated, for example, due to human error or neglect, but were not identified as changes from the baseline. Further, for entities subject to the

Sarbanes-Oxley Act, sufficient testing is necessary to support management's annual assessment of the effectiveness of internal control.

Enclosure I provides GAO's responses to the specific questions on your online comment form.

We thank you for considering our comments on this important guidance and would be pleased to discuss them with you in further detail.

Sincerely yours,

A handwritten signature in black ink, appearing to read "D. M. Walker", with a long horizontal line extending to the right.

David M. Walker
Comptroller General
of the United States

Enclosure

cc: Mr. James M. Sylph, Technical Director
International Auditing and Assurance Standards Board

The Honorable Christopher Cox, Chairman
Securities and Exchange Commission

The Honorable Mark W. Olson, Chairman
Public Company Accounting Oversight Board

Mr. Harold Monk, Chair
Auditing Standards Board

**COSO Guidance on Monitoring Internal Control Systems
Public Comment Form – Fall 2007**

Thank you in advance for providing feedback on COSO's discussion document, *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 flow of the discussion document and is appended by a few demographic questions that we will use in grouping the responses. *We would like to receive all comments by October 31, 2007.*

You can provide feedback in one of three ways. The preferred method is through a Web-based version of this form, which can be opened and completed directly via the Internet using the appropriate link on the COSO Web site (<http://www.coso.org/publications.htm>). Alternatively, you can complete the Microsoft Word version below, and email the completed form to COSOMonitoring@gt.com, or fax it to COSO Monitoring Project at (704) 337-2979. The third option is to email or fax a comment letter. 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

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?

Somewhat

Comments:

Please see GAO comment letter dated November 2, 2007.

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

Somewhat

Comments:

We propose two additional characteristics to distinguish monitoring activities from control activities, namely whether (1) the persons performing the activity understand that their responsibilities include determining whether internal controls are operating effectively, and (2) the activity has been effective in identifying control weaknesses in the past.

3. Additional comments regarding Section I.

Comments:

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

Comments:

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?

Somewhat

Comments:

We are concerned that this discussion places too much emphasis on monitoring changes in internal control rather than talking a holistic approach by focusing on control effectiveness. Conceptually, this approach could lead to no monitoring if no changes in internal control are identified.

Also, please see GAO comment letter dated November 2, 2007.

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

Comments:

We suggest the draft document include a statement that the control components the board/audit committee can monitor most effectively are the control environment and risk assessment.

- 7. Additional comments regarding Section II.

Comments:

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

Comments:

- 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

Comments:

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

Comments:

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

Somewhat

Comments:

Please see GAO comment letter dated November 2, 2007.

While the distinctions between direct and indirect information are helpful, we are concerned that the extensive discussion on indirect information, when taken together with the other factors discussed in the GAO comment letter, may lead evaluators to place greater reliance on indirect information than is warranted to support a conclusion on the effectiveness of internal control. As the draft document notes, indirect information as a basis for control assessments is less persuasive than direct information. Our concern is not whether indirect information can be used but the degree of reliance placed on this information.

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

Somewhat

Comments:

The explanation of the term "accurate" should reflect the practical consideration that information that is less than 100 percent accurate may be useful.

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

Somewhat

Comments:

This discussion does not adequately distinguish between the concepts of frequency of monitoring and timeliness of information. It should be clarified to state that timeliness refers to information that arises out of the monitoring activity and hence is dependent on the frequency of the monitoring activity.

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?

Somewhat

Comments:

This document should be expanded to include a discussion on determining whether enough suitable information has been gathered that will allow management to draw statistically defensible conclusions when testing entails sampling less than 100 percent of a population.

The document should also clarify how management should monitor the effectiveness of automated controls. For example, the table on page 17 states under "Possible Impact on the Amount of Information" for Automated Controls that "Automated controls generally operate consistently. Therefore, a periodic reconfirmation through evaluation of a single instance of automated controls is often an acceptable monitoring threshold. In such situations, management includes in its monitoring procedures the effectiveness of its program testing, program security, and change-control processes."

This may imply that Information Technology (IT) application controls do not require frequent monitoring. While this may be true for application controls in smaller, centralized PC-based environments, it is not so for more complex environments. For example, organizations using enterprise resource planning applications with many users typically require frequent monitoring of access controls to ensure access rights to application functions operate effectively and avoid segregation of duties conflicts or incompatible duties. Also because user-defined processing (e.g., spreadsheets, management reporting systems) can result in significant risk of error or fraud, monitoring of related controls generally should occur more frequently.

Additionally, the document should clarify how management should monitor the effectiveness of general controls. The Federal government has issued guidance on management's testing of internal control over financial reporting, including IT general controls, which is incorporated in the Financial Audit Manual issued jointly by the Government Accountability

Office (GAO) and the President’s Council on Integrity and Efficiency and in our Federal Information System Controls Audit Manual.

- 15. Additional comments regarding Section III.

Comments:

Section IV. Designing Effective Monitoring

- 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?

Somewhat

Comments:

Please see GAO comment letter dated November 2, 2007.

- 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?

Somewhat

Comments:

These subsections could benefit from additional examples.

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

Comments:

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

Yes

Comments:

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?

Somewhat

Comments:

This bulleted discussion on the focus of monitoring tools should be clarified so the reader understands whether control activities or monitoring controls are being discussed. In addition, COSO should consider further expanding the description of available tools, perhaps in an appendix or based on what it finds in its field visits in the next phase of the study.

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?

Somewhat

Comments:

Please see GAO comment letter dated November 2, 2007.

Also, this section should be expanded to include more details and examples, since it appears to be only an overview.

22. Additional comments regarding Section IV.

Comments:

Section V. Communicating and Addressing the Results of Monitoring

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

Comments:

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

Somewhat

Comments:

Please see GAO comment letter dated November 2, 2007.

25. Additional comments regarding Section V.

Comments:

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?

Somewhat

Comments:

The scalability discussion could benefit from inclusion of examples from small companies and less complex companies.

Other General Areas/Topics

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

Yes

Comments:

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?

No

Comments:

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

Comments:

We believe the terms "board of directors" and "audit committee" should be replaced with "those charged with governance," to use terminology that is consistent with the terminology used by other standard setters (IAASB, AICPA, GAO) and to recognize that many entities, e.g. in government, do not have a board or an audit committee.

On page v, we suggest replacing "significant" with "magnitude" to be consistent with terminology used by other standard setters (AICPA, PCAOB).

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

Comments:

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

Yes

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

Comments:

Demographic Information ---

33. Your name

David M. Walker

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

Other (please describe)

Comptroller General of the United States

35. Country

United States

36. Name of organization (should correspond to position selected in Question 34 above)

United States Government Accountability Office

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

Government agency

38. Annual revenues of the above-named organization

N/A

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

N/A