Current Issues in Auditing
Volume 7, Issue 1
2013
Pages C30–C33

American Accounting Association
DOI: 10.2308/ciia-50475

COMMENTARY

Comments by the Auditing Standards Committee of the Auditing Section of the American Accounting Association on the COSO request for comments on *Internal Control over External Financial Reporting: Compendium of Approaches and Examples*

Participating Committee Members and Other Contributors:
Karen A. Kitching, Mikhail Pevzner, and Nathaniel M. Stephens

SUMMARY: On September 18, 2012, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) solicited public comments on its exposure draft of the document entitled *Internal Control over External Financial Reporting: Compendium of Approaches and Examples* (Compendium). According to COSO's press release, the Compendium is part of its project to update the *Internal Control—Integrated Framework* (Framework) and is meant to "assist users when applying the Framework to external financial reporting objectives." The 63-day comment period ended on November 20, 2012. This commentary summarizes the contributors' views on this exposure draft (the exposure draft and other related information can be accessed at: http://www.pwc.com/us/en/cfodirect/publications/in-brief/2012-43-coso-releases-internal-control-compendium-for-public.jhtml and the associated updated Framework. Comments are separated into two sections: general comments, and comments in response to specific questions posed by COSO in its request for feedback.

Dear COSO Board Members:

The Auditing Standards Committee of the Auditing Section of the American Accounting Association is pleased to provide comments in response to your recent Invitation to Comment on

Karen A. Kitching is an Associate Professor at George Mason University, Mikhail Pevzner is an Associate Professor at the University of Baltimore, and Nathaniel M. Stephens is an Assistant Professor at Utah State University.

Submitted: January 2013
Accepted: April 2013
Published Online: April 2013

the exposure draft entitled *Internal Control over External Financial Reporting: Compendium of Approaches and Examples*.

The views expressed in this letter are those of the members of the Auditing Standards Committee and do not reflect an official position of the American Accounting Association. In addition, the comments reflect the overall consensus view of the Committee, not necessarily the views of every individual member.

We hope that our attached comments and suggestions are helpful and will assist the Board. If the Board has any questions about our input, please feel free to contact our committee chair for any follow-up.

Respectfully submitted,

Auditing Standards Committee
Auditing Section—American Accounting Association

GENERAL COMMENTS ON CONTROL ACTIVITIES OVER TECHNOLOGY

The formalization of fundamental concepts in the Exposure Draft as principles is touted as a significant change in the COSO Framework. According to the COSO Framework, the main purpose is to provide clarity for users in designing and implementing systems of internal control while not being "overly prescriptive." While it is more detailed than the original Framework, it does not provide enough guidance. Specifically, we posit that it is not sufficiently prescriptive as it relates to control activities over technology. The proposed concept changes lag behind the current state of accounting and auditing, where technology drives the recording, maintaining, and reporting of financial and nonfinancial information in all organizations.

We agree with the following statement: "No two entities will, or should, have the same system of internal controls. Entities, objectives, and systems of internal control differ dramatically by industry and regulatory environment, as well as by internal considerations such as the size, nature of the management operating model, tolerance for risk, *reliance on technology*, and competence and number of personnel" (page 6, paragraph 41; emphasis added). However, the lack of more specific guidance relating to internal controls over information technology is not justified based on varying needs. Most organizations—and all organizations that have more than a few employees—capture operating events using technology, and most are recorded in real time, not using after-the-fact batch processing, as in the past. Preventive controls easily can and should be embedded in the business processes. More detailed control requirements related to information technology should be included in the Framework.

The orientation of the Control Objectives for Information and Related Technologies (COBIT) Framework (Information Systems Audit and Control Association [ISACA] 2012) is structured around business processes. It is authoritative, relevant, and prescriptive, and it is not platform-dependent. The Information Systems Audit and Control Association (ISACA) updates COBIT every three years and provides continuous amendments to reflect technology changes. The COSO Framework, however, makes no mention of COBIT. At the very least, a direct reference for organizations to follow these guidelines should be made if none is provided within the Framework itself. Similarly, the International Organization for Standardization (ISO) establishes guidelines for implementing and maintaining information security management in an organization. In particular, ISO/IEC 27002:2005 contains best practices for control objectives and controls in many areas, including operations management, access control, and information systems

development and maintenance (ISO/IEC 2005). The COSO Framework mentions ISO/IEC 27002 when stating that organizations without an internal audit group "may periodically evaluate the entity's compliance with ISO/IEC 27002." Similar to referencing COBIT, the COSO Framework should require compliance with the ISO standards.

Supposedly, access to the information system and control activities over technology are considered in more detail under the Security Management Processes section of Principle 11. This section of the COSO Framework also falls short in providing clarity. At a minimum, separation of duties between information technology and operating functions should be delineated. Accounting should be separated from the individuals involved in the performance of operating activities, and separation of duties also is necessary for those performing IT functions. Further, accounting and IT functions should be separated. Finally, within the IT department specifically, activities should be separated, from systems analysis to data control. This type of general discussion of separation of duties is necessary for users designing and implementing systems of internal control over technology, and is not considered "overly prescriptive."

Below are comments on selected questions posed by COSO in its solicitation for feedback.

8. The *ICEFR* document will impose additional burdens on entities' reporting on the effectiveness of internal control—e.g., reporting on internal control over financial reporting based on Sarbanes-Oxley Act of 2002 (SOX) requirements.

We believe that this is a possibility, as described in the comment below:

a. If you believe that there is an additional burden, what would that be and how would it impact your organization?

A risk exists that the exposure draft might be viewed as the final word on implementation of the principles outlined in the Framework. The introduction to the Compendium is clear that other approaches could be acceptable dependent upon circumstances. However, to the extent that users of the Compendium or the external auditors who audit entities' systems of internal control view this document as a benchmark rather than as a non-comprehensive tool for implementation, the users may wind up performing non-essential work by moving from an acceptable implementation approach not included in the Compendium to an approach that is included in the Compendium.

9. The *ICEFR* document is relevant for both larger and smaller entities

While the exposure draft is relevant for both large and small entities, smaller entities likely will gain the greatest benefit from this document. Larger entities have spent significant resources of time and money in the design and implementation of strong systems of internal control, particularly since the passage of SOX. These larger entities' controls over financial reporting have been subject to external audits by independent auditors, as well as quarterly reviews by the entity as required by SOX Sections 404 and 302, respectively. With ten years of entity review and eight years of external audits of internal control, the control systems of accelerated filers are likely to be quite established and thorough at this point.[1] Thus, while larger entities may use this document to look for any potential gaps in their current systems of internal control, it is not likely to have a significant impact. However, smaller entities, whose controls have not been subject to the same

[1] This point is evidenced by the decrease in SOX 404 adverse opinions over time. For example, Audit Analytics reports in its *SOX 404 Dashboard: Year 6 Update* that while 16.9 percent of SOX 404 opinions filed during the first year of compliance were adverse opinions, only 4.9 percent of SOX 404 opinions were adverse opinions in the fifth year (Audit Analytics 2010).

level of scrutiny over the past ten years, likely would benefit more from the detailed approaches and examples provided in the Compendium as they seek to improve their internal control systems and as they transition from the prior version of the Framework to the new version.

11. The *ICEFR* document's approaches and examples clearly illustrate principles set out in the Framework.

The presentation is much clearer than its predecessor, *Internal Control—Integrated Framework: Evaluation Tools*, published by COSO in September 1992 (COSO 1992). The chapter summaries, principles, and tables summarizing principles and approaches make this Compendium much easier to use than its predecessor.

12. Additional approaches and/or examples are needed to illustrate the principles.

The committee is concerned with the amount of detail that the exposure draft provides. In fact, if judgment is valuable in improving the quality of internal control systems (as is stated in the Framework), it is difficult to understand why *so much* detail is provided.

13. Other comments on the *ICEFR* document.

While the Compendium is a valuable tool in the hands of companies that will rely on the COSO Framework in developing strong systems of internal control, it has the potential to lead to comparability at the expense of quality controls. For example, some prior research indicates that decision aids in auditing contexts may cause decision aid users to approach tasks mechanistically rather than becoming involved in the task judgmentally (Glover et al. 1997). In this context, there is a risk that users of the Compendium may over-rely on the approaches and/or examples provided, rather than critically think about the best way to incorporate the principles into their own systems of internal control. Clearly outlining the five components of internal control and the supporting principles related to each of those components and leaving the application to the users may cause Framework users to create better, custom-made approaches to incorporating the principles into their own systems of internal control. Evidence could be gained on this issue by analyzing the use of the "Evaluation Tools" published by COSO in September 1992 (COSO 1992). The Framework itself indicates that judgment "enhances management's ability to make better decisions about internal control." If that is the case, it seems counter-intuitive to provide a detailed Framework (which seems to be an expansion in detail from the previous version of the Framework), as well as specific implementation guidance in the form of this Compendium.

REFERENCES

Audit Analytics. 2010. SOX 404 dashboard: Year 6 update. Available at: http://www.complianceweek.com/s/documents/AASOX404.pdf

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control—Integrated Framework Evaluation Tools*. New York, NY: COSO.

Glover, S. M., D. F. Prawitt, and B. C. Spilker. 1997. The influence of decision aids on user behavior: Implications for knowledge acquisition and inappropriate reliance. *Organizational Behavior and Human Decision Processes* 72 (2): 232–255.

Information Systems Audit and Control Association (ISACA). 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: ISACA.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). 2005. *Information Technology, Security Techniques, Code of Practice for Information Security Management*. ISO/IEC 27002:2005(E). Geneva, Switzerland: ISO/IEC.