
SEC FLASH REPORT

COSO Issues New Guidance for Smaller Public Companies

July 13, 2006

On July 11, 2006, the Securities and Exchange Commission (SEC) published a Concept Release as a prelude to its forthcoming management guidance on the evaluation of internal control over financial reporting (ICFR). In addition, on that same day, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its guidance on the application of the *Internal Control – Integrated Framework* to smaller companies. This Flash Report provides an overview of the latest guidance issued by COSO. A separate Flash Report summarizes the purpose and focus of the SEC's Concept Release. BOTH of these developments are important because they represent the specific input the SEC indicated it would consider prior to finalizing its guidance to management related to the requirements for public companies to perform an assessment of the effectiveness of ICFR in accordance with The Sarbanes-Oxley Act of 2002 (SOA).

COSO's new guidance, entitled *Internal Control over Financial Reporting – Guidance for Small Public Companies*, was developed at the SEC's request to make the *Internal Control – Integrated Framework*, issued in 1992, easier and more cost-effective for smaller companies to apply. The 1992 framework is the standard of choice among large U.S. public companies, many of which have complied with SOA for two years. Smaller companies, however, have raised concerns that the original framework does not provide sufficient guidance for application to their unique circumstances. These smaller companies – the nonaccelerated filers – don't begin complying with Section 404 of SOA until next year.

In conjunction with the release of its new guidance, COSO sponsored a panel discussion on July 11, 2006, that provided (a) an overview of the new COSO document, (b) suggestions on how to use the new guidance, and (c) observations on the perspectives of smaller company management, the independent auditor and the internal auditor. The panel was moderated by Dave Richards, President of The Institute of Internal Auditors and included participation by Larry Rittenberg, the Chairman of COSO, as well as others.

Overview of the COSO Document

COSO's new guidance was developed in response to a request by the Chief Accountant of the SEC. As outlined by Larry Rittenberg, the objectives and purpose of the new guidance are twofold:

- Articulate better the fundamental principles of internal control for use by smaller companies
- Provide practical examples illustrating application of the principles in a smaller company environment.

The original 1992 *Internal Control – Integrated Framework* remains intact. The new guidance does not supersede it. The new guidance is based on the original framework and clarifies the framework's fundamental principles.

COSO's overall focus to this project was to develop principles-based guidance. The emphasis on principle-based guidance suggests the following:

- Management judgment is a pre-requisite to any evaluation of the effectiveness of internal control. Management must make decisions on the best way to implement internal control. Therefore, only management can decide the critical controls to document, evaluate and test.
- There is no "one-size-fits-all" approach, because there are alternatives in how to implement effective internal control. Because the new guidance is not a cookbook, management still needs to make decisions.
- Effective internal control is a continuous process. Therefore, it is important to focus on improvement and efficiency.
- The five components of internal controls are interrelated. All five components are important within a continuous process of achieving effective internal control.
- It is important to focus on the objectives of internal control. The guidance provides 20 core principles as well as attributes of those principles. The 20 principles are summarized in the attached *EXHIBIT* at the end of this Flash Report. The principles provide guidance for evaluating the five internal control components. The attributes provide guidance for evaluating the principles.

The guidance addresses tough issues commonly experienced in smaller companies. These issues include documentation, segregation of duties, management override and the increased role and importance of effective monitoring. The examples provided in the guidance are based on actual experiences of a smaller company.

How to Use the Guidance

The guidance consists of three volumes:

- Volume I is an Executive Summary. The intended audience for this volume is the Board, Audit Committee and senior management. It summarizes recent developments, internal control challenges, and the costs and benefits associated with internal control. It focuses on risk as a basis for designing effective internal controls and introduces the discussion of internal control as a process.
- Volume II is the guidance volume. This is the largest of the three volumes. The intended audience is senior management and management involved in the design, implementation and operation of internal controls. It provides an overview of ICFR in smaller businesses and discusses the costs and benefits of internal control, how companies can meet the challenges of attaining cost-effective internal control and provides other considerations for achieving further efficiencies. Volume II focuses on the aforementioned 20 fundamental principles drawn from the original 1992 *Internal Control – Integrated Framework* (Framework). These principles assist smaller businesses in achieving internal control in a cost-effective manner.

Volume II details principles, attributes, approaches, and examples:

- Principles are fundamental concepts associated with effective internal control over financial reporting and are drawn directly from the five components of the Framework.
 - Attributes are characteristics associated with a given principle and clarify how to evaluate that principle.
 - Approaches describe how smaller companies can apply a given principle.
 - Examples illustrate how the approaches can be used to apply a principle. As with the approaches, each example is referenced to related attributes, which may be useful in considering how best to achieve the principle.
- Volume III contains the evaluation tools. Management may use some, all or none of these tools. The intended audience is management and others that have been requested to evaluate and help senior management evaluate the effectiveness of ICFR. It contains illustrative tools to assist management in the internal control evaluation process. Managers may use the illustrative tools in determining whether the company has effectively applied the principles.

The Small Company Perspective

The new guidance is expected to help smaller companies by (a) focusing on specific principles and attributes that are aligned with the five components outlined in the 1992 COSO *Internal Control – Integrated Framework*, and (b) providing illustrative approaches and examples. Volumes II and III illustrate how small businesses have actually implemented the principles and the related attributes. While the examples are not meant to be checklists, COSO believes they will be helpful to management of smaller companies in determining the approach and level of documentation. All examples are from actual small company situations and help demonstrate how controls function in a small business environment.

An effective risk assessment process is vital to achieving cost-effective internal control. The guidance provides robust examples of how to conduct an effective risk assessment to help control costs, identify the appropriate level of internal controls and manage technology-related issues. For example, the guidance gives examples and approaches on dealing with challenges common in small businesses:

- Resources (segregation of duties), i.e., in a smaller company, the answer can't always be "add more resources"; therefore, the guidance provides examples of developing alternative controls
- Management domination
- Board committee membership
- Qualified accounting personnel
- Information technology
- Documentation (the guidance provides templates that smaller companies can use to assist them in designing and implementing controls)

The guidance enables management and the Board to make smarter decisions regarding the types of controls necessary and the level of control required to support financial reporting objectives when considering the organization's complexity. The organization's complexity is impacted by such variables as transaction complexity, dispersion of operations, and sophistication of computer applications and systems.

The guidance also enables the organization to design and implement internal controls effectively and efficiently by designing and implementing only those important controls that are right-sized for a smaller public company. Again, while not a cookbook, the tools and templates included in Volume III will assist small companies in their documentation efforts.

The External Auditor's Perspective

With respect to the expected benefits to the independent auditor, the latest COSO guidance and tools will benefit the attestation process for smaller public companies and generate efficiencies as follows:

- Historically there have been disconnects between the auditors and management as to the “key controls.” COSO expects that the new guidance will encourage and facilitate more auditor-management agreement on the appropriate controls.
- The guidance is expected to foster greater consistency of COSO principles-based application across companies and across industries. Because of this expected consistency, auditors will become more efficient as they observe similar controls in operation across companies and industries.
- The new guidance will encourage greater consistency in the format and scope of company documentation. Companies applying the guidance will be more consistent in executing the risk assessment process and how they document their controls. This consistency will enable increased efficiency in incorporating risk assessments into the auditors’ evaluation.

Because not all "small" companies are created alike, COSO doesn't draw bright lines around what a small company is. It ultimately depends on the complexity of the company. Therefore, the characteristics of some “small companies” will impact the degree of efficiencies to be gained. These characteristics include:

- Degree to which management applies the guidance and exhibits the proper tone-from-the-top
- Degree of accounting complexity (by choice or by industry)
- Degree of centralization vs. decentralization
- Degree of geographic diversity

During the panel discussion, it was observed that companies can take steps to maximize the possible auditor efficiencies by ensuring that:

- They approach the evaluation of ICFR seriously;
- They perform a proper risk assessment focused on material accounts and disclosures, critical financial statement assertions and key control objectives;
- They operate company-level controls at an *appropriate level of precision* (e.g., annual budget-to-actual comparisons probably aren't enough; monitoring controls need to operate at a level of precision to provide reasonable assurance that a material error in the financial statements would be detected before the financials are published); and

- They stick to business transactions that are commensurate with the company's size and skills

The Internal Auditor Perspective

The COSO Framework can be used in many ways by internal auditors, according to Dave Richards. For example, it can be used as a training resource, as a framework for designing internal control and in preparing audit programs to test internal controls in specific areas. The tools provided in the guidance can also help internal auditors assess internal controls. The guidance can be a reference point for summarizing and communicating results of internal audits to ensure all important aspects are addressed. The guidance fosters consistent audits because it provides common assessment criteria across multiple processes and audit areas.

Some Common Themes from the COSO Panel Discussion

During the COSO-sponsored panel discussion, several common themes emerged from the prepared remarks and the Q&A dialogue. These common themes are summarized below:

- The final guidance differs from the exposure draft in several ways. First, the exposure draft had 26 principles, and the final guidance has 20 principles. Second, the final guidance places more focus on cost effectiveness. Third, the final guidance is packaged into three volumes based on the intended audience. COSO believes the final document is more user-friendly than the exposure draft. For example, the final guidance includes a color-coding system that matches specific compliance elements to the relevant principles and attributes.
- It is generally expected that companies must address all 20 of the fundamental principles. If all 20 principles are not addressed, management must evaluate the impact of not having them all present. While the failure to address a specific principle may be indicative of a significant deficiency or a material weakness, it is not automatically classified at a level of being more than a control deficiency. The same is true of attributes, which are generally associated with a given principle. Therefore, companies don't necessarily need every attribute in place to conclude that a principle is sufficiently addressed and operating effectively.
- The examples and tools included in Volume III are not meant to be prescriptive and they are not checklists. Management must tailor the examples to the specific facts and circumstances based on an assessment of the attributes germane to the specific principles as applied to the organization. The cost of complying with the COSO framework is dependent on the complexity of the organization, the technology used, the number of

locations, and other factors. Implementing internal controls may be more cost-effective if controls are built into the process as opposed to making controls an “add-on” to the process.

- The guidance emphasizes that documentation for smaller businesses can be less formal. However, the guidance doesn’t fully clarify or resolve the issue of providing documentation for auditors. To provide evidence for assertions to third parties (i.e., the external auditor), there needs to be a minimum level of documentation regardless of the informality of the controls in place. The auditor needs something to audit because the auditor isn’t always present to observe the controls in operation. The auditor needs more evidence than simply inquiring of senior management as to whether the controls are working. The audit requirement will continue to have an impact on the cost of the compliance process.
- Many smaller companies already have good internal controls. Internal controls mitigate the risk of failure and help companies succeed. They are an integral part of a well run business and are not an add-on to essential business processes. That said, there is generally a greater risk of error in financial reporting in smaller public companies. The point was made during the panel discussion that the SEC and Congress (and not COSO) are the bodies with the authority to consider “exemptions” or other relief for smaller companies.
- The risk of management override and fraud is an extremely important consideration in financial reporting. The guidance provides practical examples related to fraud issues. The guidance points out that fraud risk should be considered throughout the risk assessment and should be integrated into control activities.
- With respect to IT controls for smaller companies, the 1992 framework didn’t address IT in a robust manner. Volumes II and III of the new guidance advance the point of view that IT should be embedded in risk assessment because all controls are impacted by technology. Therefore, involving IT is extremely important to the design of effective controls and to help reduce costs. Volumes II and III provide examples and templates about how to assess risk and design appropriate IT general and application controls. The guidance includes examples for a less complex and a more complex IT environment. It is important to understand that a so-called “smaller company” doesn’t necessarily have a less complex technology environment. Therefore, the guidance focuses not on size, but on the complexity of the technology environment.

In addition to the above common themes, two other important points were raised:

- The principles outlined in the guidance are based on financial reporting and are sound regardless of the organization's structure. While there is some discussion specific to Section 404, the principles, attributes and examples can be applied to not-for-profit and non-public companies. The principles, attributes and examples should also be valuable for larger businesses.
- COSO recognizes the need for more continued guidance in specific risk and control areas and the need to address several important topics such as what constitutes effective monitoring and continuing risk assessment. COSO also intends to highlight the importance of its *Enterprise Risk Management – Integrated Framework*.

Summary

In summary, COSO has released the Executive Summary and a Frequently Asked Questions document (which includes 27 questions). Interested parties can obtain these documents at <http://www.coso.org/publications.htm>. Interested parties can also order the complete three volume guidance at the following AICPA website: <https://www.cpa2biz.com/stores/coso3> (which is also linked to the COSO site). The three volume set includes the Executive Summary as Volume I.

Twenty basic principles outlined by COSO as the fundamental concepts necessary to achieving effective ICFR

CONTROL ENVIRONMENT

- (1) **Integrity and Ethical Values.** Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.
- (2) **Board of Directors.** The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.
- (3) **Management's Philosophy and Operating Style.** Management's philosophy and operating style support achieving effective ICFR.
- (4) **Organizational Structure.** The company's organizational structure supports effective ICFR.
- (5) **Financial Reporting Competencies.** The company retains individuals competent in financial reporting and related oversight roles.
- (6) **Authority and Responsibility.** Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective ICFR.
- (7) **Human Resources.** Human resource policies and practices are designed and implemented to facilitate effective ICFR.

RISK ASSESSMENT

- (8) **Financial Reporting Objectives.** Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.
- (9) **Financial Reporting Risks.** The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.
- (10) **Fraud Risk.** The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

CONTROL ACTIVITIES

- (11) **Integration with Risk Assessment.** Actions are taken to address risks to the achievement of financial reporting objectives.
- (12) **Selection and Development of Control Activities.** Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives.
- (13) **Policies and Procedures.** Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.
- (14) **Information Technology.** Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

INFORMATION AND COMMUNICATION

- (15) **Financial Reporting Information.** Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.
- (16) **Internal Control Information.** Information used to execute other control components is identified, captured, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.
- (17) **Internal Communication.** Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.
- (18) **External Communication.** Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

MONITORING

- (19) **Ongoing and Separate Evaluations.** Ongoing and/or separate evaluations enable management to determine whether ICFR is present and functioning
- (20) **Reporting Deficiencies.** Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.