



LEADING THE IT GOVERNANCE COMMUNITY

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 January 2006

COSO Board

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

Also submitted via online questionnaire

RE: *Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting* Exposure Draft

Dear COSO Board:

Congratulations on the issuance of the exposure draft, *Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting* (“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 the 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 56,000 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 focus is well placed and the information is pragmatic and practical, lending itself to immediate and direct use within most enterprises.

We do have concern regarding the ability of some very small public companies (e.g., many of those "micro cap" companies in the bottom 1 percent of market capitalization) to apply the recommended principles effectively. In many of these situations:

- Boards of directors may not have independent critical mass nor an audit committee with sufficient financial and IT expertise.
- There is a limited pool of employees in the accounting and IT functions, thereby limiting financial reporting expertise and making segregation of duties difficult.
- There is no internal audit function.
- The control environment may be positive, but often it is informal.
- Many job descriptions, policies and procedures are not formally documented.
- Internal control over financial reporting is often a function of hands-on involvement by senior management in the day-to-day operations of the business and management's use of budgets, which enables them to predict revenue, costs and important balance sheet amounts.

Recommendation: *Introduce a three-tier stratification (such as the one recommended by the SEC Advisory Committee on Smaller Public Companies), which recognizes that some "micro cap" companies may have internal controls with limited effectiveness.*

Primary Comments

Our primary comments focus on the following areas:

- Board and management responsibility
- Importance of budgets
- Complexity of systems
- Cost-effective IT controls for smaller companies
- Continuous monitoring

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.

Board and Management Responsibility

Sufficient board and senior management involvement in IT is needed for an effective control environment. The tone at the top should reflect good IT governance and require that IT appear regularly on the board agenda. We believe that as board and senior management involvement with IT matters increases, IT-related risks are reduced and IT controls become more effective.

Recommendation: *Include guidance about how senior management and the board of directors can increase their involvement in IT governance matters. For example, the board should meet regularly (at least annually) with IT management to review systems plans, performance, risk analyses, outsourcing and security issues and their effects on internal control over financial reporting.*

Aspects of this recommendation should be incorporated as an attribute of the Importance of Board of Directors Principle on page 29 and smaller company approaches under the Board Communication Principle on page 103. This recommendation also supports the risk assessment approach on page 54.

In addition, as with the COSO *Internal Control—Integrated Framework* itself, the board might consider addressing the topic of IT governance beyond those aspects relevant to financial reporting. It is our experience that those organizations that implement a broad set of IT governance principles are the ones that receive the highest cost/benefit from controls. This is an especially important benefit in smaller companies. In this regard, reference could be made to the IT Governance Institute publication *Board Briefing on IT Governance, 2nd Edition*.

Importance of Budgets

Budgets are an especially important control in smaller companies; however, this concept is treated inconsistently in the draft. For example:

- On the bottom of page 15, the bullet “A less effective compensating control” relates to budget review and trend analysis.
- On page 16, the wording of the bullet seems to convey an unintended message that growing the business is more important than spending time performing operational aspects of financial reporting. While we do not disagree that growing the business is indeed important, even critical, it cannot or should not be done to the exclusion of performing proper financial reporting, and *vice versa*.
- The budget review is given more value on page 67 in Control Activities.

Recommendation: Remove the inconsistencies and re-emphasize the concept that management participation in the development of the budget for strategic/operational planning purposes and management review of the operating results against the budget can be effective controls in a smaller business.

Complexity of Systems

The language describing information technology, starting at the bottom of page 18, is an oversimplification of the issues and could be misleading. It implies that the use of packaged software requires fewer controls than custom, in-house developed software. It ignores issues such as:

- Complexity of the processing
- Degree to which packaged software is user-configurable
- Use of packaged software customized by third parties

Recommendation: Revise the wording at the bottom of page 18 to read: *The level of effort required to establish effective internal control over information technology is largely, although not completely, a reflection of (1) the degree of complexity of the transaction processing of the computer systems and (2) the type(s) of software used in the financial and accounting systems of the enterprise. The degree of complexity can be described somewhat as follows:*

- *Simple Transaction Processing Systems—Those systems that process accounting and*

financial transactions where input controls can be easily reconciled to the output of the systems

- *Complex Transaction Processing Systems—Those systems that process accounting and financial transactions where the software requires the periodic input of data used in initiating transactions, calculating or modifying information in the system, and where it is not possible to easily reconcile input to the output of the systems. Such accounting systems require greater reliance on the software to generate accounting information and, thus, require greater reliance on IT controls.*

The types of software can be described somewhat as follows:

- *Prepackaged accounting software—Can be fairly standard in its functions with few processing options or can be highly configurable by the enterprise by specifying, from a range of processing options and controls, the particular functionality required. Software that is configurable requires a greater degree of IT control than software with few processing options.*
- *Customized software—Packaged software that is modified or supplemented to meet the processing needs of the enterprise. Often this type of software requires updating and additional modification as additional features are provided or the needs of the enterprise change. Programming is typically performed by third parties but may be installed by enterprise personnel. This process requires IT change management controls to ensure that updates and modifications process financial information reliably.*
- *In-house developed software—Requires IT systems development controls in addition to IT change management controls to ensure that systems function as intended and process financial information reliably.*

The degree of access controls and supporting information security infrastructure depends on the functionality, complexity and configurability of the financial systems.

Also, add an example on page 18 or on page 57 along the following lines to illustrate what can go wrong in a complex processing system.

Risks in a Complex Processing System

A complex system is one that processes accounting and financial transactions and requires the periodic input of data used in initiating transactions, calculating or modifying information in the system, and in which it is not possible to easily reconcile input to the output of the system.

A multimillion-dollar company has as its business focus, and profits from, the difference between the interest it earns and the cost of debt issued to fund the purchases of debt. Some of the paper it keeps for resale and some it keeps on its books. The company runs a number of complex systems, and has a few packages, but the vast majority is custom, in-house developed systems. The company operates all over the US.

The company reported it had to lower net income significantly because of a computer error. The computer glitch delayed its quarter-end earnings release, and the entire financial reporting was adversely impacted. The company discovered that a technology program developed several years

ago was overvaluing interest income accrued on securities backed primarily by variable-rate loans the company purchased from private issuers. Because of this error, the company had to begin looking at many other computer internal applications, both home-grown and packaged systems, to ensure there were not other programming functionality issues in its other systems.

Cost-effective IT Controls for Smaller Companies

Enterprises should clearly assign responsibilities for important IT control activities, such as security, change management and operations controls. Although in larger companies these might be full-time responsibilities, in smaller companies persons with control responsibilities frequently have other duties as well and they also may share these responsibilities with others.

Recommendations:

On page 81, add an attribute of the principle along the following lines “Enterprises should clearly assign responsibilities for important IT control activities.”

Also, add an example along the following lines to page 86 or 87 to illustrate this concept.

Assigning IT Control Responsibilities

A \$180 million in sales wholesale and retail consumer products company with a relatively high degree of automation has a six-person IT staff and a six-person accounting department. They address IT security controls by assigning these responsibilities to two individuals who also have other responsibilities.

- The IT network manager is assigned the responsibility for IT security. This individual attends training by ISACA and reviews security products, such as firewalls, and security aspects of packaged software, such as access security and password change controls. He is responsible for recommending security policies and practices, which he drafts for review and approval, and is the owner of the IT security policy. He also is the key manager for backup and recovery.
- The assistant controller is assigned the responsibility for approving access to the IT system. These responsibilities include, among other responsibilities, the documented sign-off approving access to applications or certain functions within applications before IT provides access to the systems.

The material contained on pages 81-90 and in appendix D provides some very good guidance to the management of smaller business enterprises. Just as the COSO *Internal Control—Integrated Framework* is being used as a good basic methodology for considering internal control over financial reporting, we suggest that the board may want to consider either recommending or, at least, providing the reader with source material on the use of a control methodology or control framework for information technology. Although many of these frameworks address controls in addition to those that may be relevant to reliable financial reporting, use of these frameworks can often result in an effectively controlled IT environment that helps ensure reliable business operations and reliable financial reporting in a cost-effective manner.

Recommendation: *Recommend or, at least, provide the reader with source material on the*

use of a control methodology for information technology, such as COBIT Quickstart (IT Governance Institute, 2004), IT Control Objectives for Sarbanes-Oxley (IT Governance Institute, 2004) or Information Technology Code of Practice for Information Security Management—ISO/IEC 17799 (International Organization for Standardization/International Electrotechnical Commission, 2005).

Continuous Monitoring and Exception Reporting

Page 20 of the exposure draft, Account Balances Are Not Just Transaction Based, presents three processes as affecting account balances: transaction processing, accounting estimates and adjusting entries (closing entries and unusual transactions, i.e., subject to management override). Furthermore, page 21 notes that most frauds occur by accounting estimates and adjusting entries. Continuous monitoring and exception reporting can be cost-effective controls for smaller companies. There are many new continuous monitoring packages and other tools that may benefit smaller companies. For example, companies can easily use data analysis software for continuous monitoring or exception reporting. Other programs can review for duplicate payments, matching shipping documents, purchase order changes and unusual transactions or adjustments. In addition, some tools can monitor segregation of duties and changes in access profiles.

***Recommendation:** Mention continuous monitoring, data analysis and exception reporting as efficient control options.*

Again, we appreciate the opportunity to comment on the exposure draft of the COSO guidance for smaller public companies. Thank you for considering our views. We would be happy to discuss them with you in further detail.

Respectfully submitted,



Everett C. Johnson, CPA
2005-2006 International President
ISACA (www.isaca.org)
IT Governance Institute (www.itgi.org)

Attachment A—Secondary Comments in Page Order

Page 2, Executive Summary, discusses smaller company expectations in the bullet, “The *control environment*... .”

Recommendation: *It would be useful to indicate in this bullet why, how or to whom management’s actions are “more transparent in small businesses than larger enterprises.”*

Page 3, Executive Summary, the bullet on *personal responsibility for controls* should reflect that most employees do not understand controls or the extent of controls needed in an environment.

Recommendation: *Include something about training in the bullet, such as: “Even smaller companies can implement effective procedures and training so that...”*

The bottom of page 4, Formalization of Controls and Documentation, in the second bullet, Management Assertion, the basic thought is that smaller companies may verbally communicate weaknesses in internal controls. In the absence of written communication, it would be beneficial to clarify how a company will determine that weaknesses have not been lost and that they have been properly communicated from one person to the next or from one level of employees to the management and then to the audit committee. However, we believe written communication should be the norm.

Recommendation: *Add: “Weakness should be appropriately documented and communicated in writing.”*

Page 21, exhibit 2.4 is an excellent depiction of the three aspects leading to financial account balances and disclosures. We suggest that the wording in the exhibit title (and the wording that precedes the exhibit) be changed from “Financial Reports” to “Financial Reporting” so the reader always relates back to exhibit 2.4 when subsequent references are made to “financial reporting,” or “internal control over financial reporting,” particularly the first two bullets on page 29.

Recommendation: *Change the wording in the exhibit title (and the wording that precedes the exhibit) from “Financial Reports” to “Financial Reporting” to agree with the use of the term “financial reporting” used extensively throughout the report.*

Page 29, Importance of Board of Directors, the list of bullets addressing Attributes of the Principle should emphasize the importance of IT expertise on the audit committee.

Recommendation: *Recommend that the following statement be added: “One or more members of the audit committee have sufficient IT understanding commensurate with the complexity of the entity’s IT systems.”*

Page 37, if the COSO board accepts the rewording as suggested in the main body of this letter in the section on Complexity of Systems, then an additional change is also suggested in the following recommendation. Note that these suggestions provide a good link to the concepts on:

- Page 57, relating to Analyzing Risk for Information Technology
- Page 60, relating to Business Process Characteristics, such as “complexity of the process”

- Pages 81-85, links more clearly to these discussions

Recommendation: *On page 37, reword the second bullet, Approaches Smaller Companies Can Take, adding the underlined words: “Significant transaction processing systems are identified as being simple or complex processes and the processes are documented to explain the flow of transactions, controls to address key risk areas, and related reporting responsibilities.”*

Page 48, Risk Assessment, first paragraph, second sentence, “Controls then act to mitigate those risks” is an incomplete risk treatment picture as described in COSO ERM.

Recommendation: *State that: “Risks can be mitigated by approaches other than internal control activities.”*

Pages 48-49, Risk Assessment, the example starting at the bottom of page 48 supports the focus only on operations and internal controls that have an effect on financial reporting. However, since “Credit Check” is included as an operational process (what seems to be the traditional credit and collection function), it might give an impression in the “Sample Company Sales Process” that an operation such as Credit Check is either not part of the financial reporting process or does not need to be considered. We realize that there is a connecting arrow between Credit Check and Product Shipment. An additional sentence at the end of the last paragraph on page 48 would provide clarity. Note that on page 63, Credit & Collections is shown as an important function within Revenue & Receivables.

Recommendation: *Add the following sentence: “Operational processes such as Credit Check in the following diagram have a dual role as being an important operating process, as well as having an important supportive effect on internal controls for financial reporting purposes.”*

Page 49, the bullet list of errors, irregularities and misstatements fails to mention duplicate recording of transactions.

Recommendation: *Reword the last bullet to read: “Recording transactions that did not exist, did not occur, or that have already been recorded.”*

Page 51 refers to a footnote 5, which does not exist.

Recommendation: *Reference should be to footnote 6 and footnotes should be renumbered.*

Page 57, Analyzing Risk for Information Technology Example seems incomplete.

Recommendation: *Add two more bullets to characterize the types of risks that might be considered and the controls designed to address such risks, such as:*

- *Information technology management then considers IT-related risks related to these critical applications and processes, such as those related to:*
 - *Security and unauthorized access*
 - *Systems processing problems*
 - *Systems interruptions*

- *Updates or changes to applications or processes.*
- *Information technology management then ensures that controls are designed and implemented to address the important risks identified.*

Page 81, Attributes of the Principle, Application controls, second sub-bullet, “authorization and validity” seem in the wrong place in this sentence.

Recommendation: *Change sub-bullet to “Designed to provide completeness, accuracy, authorization and validity of information processing ...”*

Page 81, Information Technology Attributes of the Principle, the second bullet, General Controls, refers to data backup and recovery. Generally, these types of controls do not affect the reliability of financial reporting unless there has been a significant systems interruption requiring recovery. (Data backup and recovery controls are also mentioned several other times in the document.) General Controls also refers only to access controls and physical security controls, but not to the other types of logical security controls that would normally be required.

Recommendation: *Clarify this point to avoid the implication that smaller businesses need an elaborate backup and recovery plan to meet Section 404. Revise the end of the sentence to read: “...vendor management, and logical and physical security critical to the integrity of the financial reporting process.”*

Page 82, in the fourth sub-bullet, VPN should be spelled out.

Recommendation: *Spell out virtual private network (VPN).*

Page 86, Example Using Password Access, the third bullet, “Are reset every 90 days,” is confusing.

Recommendation: *Change the bullet to read, “Are required to be changed every 90 days by the user.”*

Page 91, Information and Communication, third paragraph, the last sentence, while correct, seems out of context.

Recommendation: *Move the sentence “Top management actions can also speak louder than words in interactions with employees, customers and suppliers” to Principle 17, Management Communication on page 98, or somewhere under Control Environment.*

Page 96, the first Example of Effective Ways to Achieve the Principle title does not fit the example.

Recommendation: *Change “Updating Information Systems to Support Risk Assessment” to “Risk Assessment Considers Changes in Systems.”*

Page 97, matrix, while often used in the design of systems and controls, information maps are unlikely to be implemented retroactively by smaller companies. The inclusion of information

maps, while desirable, may result in the impression that they are required for effective internal control.

Recommendation: *This illustration needs further explanation to be useful and, if retained, should be explained and titled “Illustrative Information Map.”*

Page 106, the sub-bullet, “the intranet,” at the top of the page should be clarified.

Recommendation: *Revise the bullet to read, “The organization’s intranet.”*

Page 110, first example, Using Built-in Operating Measure and Key Control Indicators, would benefit from a second example after “accounts payable.”

Recommendation: *Add another example illustrating KCIs for IT: “In IT, for example, KCIs focus on processing problems, security incidents, successful implementation of systems updates, and user complaints.”*

Page 111, Firsthand Knowledge of the Rhythm of a Business Example does little to illustrate monitoring of internal controls over financial reporting.

Recommendation: *Include some control-related monitoring activities in the example.*

Page 112, Separate Evaluations would be easy for a reader to interpret to mean that each of the five internal control components needs to be evaluated separately from the others, which is contrary to the concept of an integrated framework.

Recommendation: *Use the terminology “objective evaluations” or similar wording to help clarify the intent.*

Page 121, Approaches Smaller Companies Can Take to Achieve the Principle could unintentionally convey the message that controls are primarily the responsibility of internal audit since four of the five bullets relate to internal audit. Internal audit should be summarized in one bullet. We believe the bullets should include other personnel in addition to internal audit, such as financial and accounting, business unit and IT professionals. It should also recognize that there are a wider array of applicable standards.

Recommendation: *Revise the section to read:*

- *The company’s annual personal goal-setting process conducted through the human resources function includes financial reporting objectives for those directly or indirectly involved in the financial reporting process. Functions affecting financial reporting that need to be involved include:*
 - *Financial and accounting*
 - *Business units*
 - *Information technology*
 - *Purchasing, human resources, treasury, legal, etc.*
- *The company has an internal audit activity that has members that are financially literate, have sufficient IT audit experience and are cross-functional employees, or has an*

outsourced internal audit function, working under the direction of the audit committee.

- *Audit work is performed in accordance with appropriate standards, such as:*
 - *Auditing standards and guidance issued by the Public Company Accounting Oversight Board*
 - *Institute of Internal Auditor International Standards for the Professional Practice of Internal Auditing*
 - *ISACA IS Auditing Standards, Guidelines and Procedures*

Attachment B—Responses to COSO Online Questionnaire

1. This document provides guidance that will help companies develop and implement internal controls over financial reporting. Somewhat Agree

As a whole, we support the board's goals for the project and the resulting draft itself, which we believe accomplishes the board's high-level objectives for most businesses. We do have concern regarding the ability of some very small public companies (e.g., many of those "micro cap companies" in the bottom 1 percent of market capitalization) to apply the recommended principles effectively.

Please see additional information on pages 1 and 2 in our letter in the section "General Comments."

2. This document will help smaller organizations strengthen their internal control processes in a more cost effective manner. Somewhat Agree

The focus is well placed and the information is pragmatic and practical, lending itself to immediate and direct use within enterprises. However, it may not be cost-effective for some very small companies.

3. This document improves my/our understanding of the Internal Control - Integrated Framework. Somewhat Agree

The COSO *Internal Control—Integrated Framework* is being used as a good basic methodology for considering internal control over financial reporting. However, the language describing information technology, starting at the bottom of page 18, is an oversimplification of the issues and could be misleading, and should be further clarified. It implies that the use of packaged software requires fewer controls than custom, in-house developed software. It ignores issues such as:

- Complexity of the processing
- Degree to which package software is user-configurable
- Use of packaged software customized by third parties

Please see additional information on pages 3 and 4 in our letter in the section "Complexity of Systems."

4. The 26 principles set out in the Guidance are sufficient for effective internal control over financial reporting. Somewhat Agree

Sufficient board and senior management involvement in IT is needed for an effective control environment. The tone at the top should reflect good IT governance and require that IT appear regularly on the board agenda.

Budgets are an especially important control in smaller companies; however, this concept is treated inconsistently in the draft.

Please see additional information on pages 2 and 3 in our letter in the sections "Board and Management Responsibility" and "Importance of Budgets."

5. There are principles in the Guidance that are not required for effective internal control over financial control- please explain in the text below. Somewhat Agree

Page 81, Attributes of the Principle Information Technology, the second bullet, General Controls, refers to data backup and recovery. Generally, these types of controls do not affect the reliability of financial reporting unless there has been a significant systems interruption requiring recovery. (Data backup and recovery controls are also mentioned several other times in the document.) General Controls also refers only to access controls and physical security controls, but not to the other types of logical security controls that would normally be required.

6. This guidance will be useful to diverse groups, including management, internal auditors and external auditors. Somewhat Agree

Enterprises should clearly assign responsibilities for important IT control activities, such as security, change management and operations controls. Although in larger companies these might be full-time responsibilities, in smaller companies persons with control responsibilities frequently have other duties as well and they also may share these responsibilities with others.

Please see additional information in our letter in the section “Cost-effective IT Controls for Smaller Companies.”

7. Are the additional examples that you believe would enhance the guidance that you can provide. If so, please indicate the related principle. The following two examples may help illustrate the principles.

Assigning IT Control Responsibilities

A \$180 million in sales wholesale and retail consumer products company with a relatively high degree of automation has a six-person IT staff and a six-person accounting department. They address IT security controls by assigning these responsibilities to two individuals who also have other responsibilities.

- The IT network manager is assigned the responsibility for IT security. This individual attends training by ISACA and reviews security products, such as firewalls, and security aspects of packaged software, such as access security and password change controls. He is responsible for recommending security policies and practices, which he drafts for review and approval, and is the owner of the IT security policy. He also is the key manager for backup and recovery.
- The assistant controller is assigned the responsibility for approving access to the IT system. These responsibilities include, among other responsibilities, the documented sign-off approving access to applications or certain functions within applications before IT provides the access to the systems.

Please see additional information in our letter in the section “Cost-effective IT Controls for Smaller Companies.”

Risks in a Complex Processing System

A complex system is one that processes accounting and financial transactions and requires the periodic input of data used in initiating transactions, calculating or modifying information in the system, and in which it is not possible to easily reconcile input to the output of the system.

A multimillion-dollar company has as its business focus, and profits from, the difference between the interest it earns and the cost of debt issued to fund the purchases of debt. Some of the paper it keeps for resale and some it keeps on its books. The company runs a number of complex systems, and has a few packages, but the vast majority is custom, in-house developed systems. The company operates all over the US.

The company reported it had to lower net income significantly because of a computer error. The computer glitch delayed its quarter-end earnings release, and the entire financial reporting was adversely impacted. The company discovered that a technology program developed several years ago was overvaluing interest income accrued on securities backed primarily by variable-rate loans the company purchased from private issuers. Because of this error, the company had to begin looking at many other computer internal applications, both home grown and packaged systems, to ensure there were not other programming functionality issues in its other systems.

Please see additional information in our letter in the section “Complexity of Systems.”

8. In helping plan for the future, are there areas where COSO can provide additional guidance?

As the COSO board is considering a longer-term plan, it would be helpful if the board would adopt a strategic planning process. As part of this process, COSO should look to:

- Provide additional guidance on IT controls
- Provide a better link between the COSO control framework and IT control frameworks and elaborate on how these work together
- Provide guidance on controls in addition to those relating to financial reporting