

January 13, 2006

Committee of Sponsoring Organizations

Submitted Electronically Through COSO Website:

<http://www.ic.coso.org/coso/cosospc.nsf/frmWebCOSOComment?OpenForm>

Sent by e-mail: COSOinternalcontrol@us.pwc.com

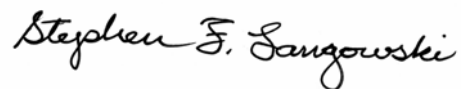
Re: COSO Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting exposure draft

To Whom It May Concern:

The New York State Society of Certified Public Accountants, the oldest state accounting association, represents approximately 30,000 CPAs that will implement the guidance proposed in its exposure draft. NYSSCPA thanks COSO for the opportunity to comment on its exposure draft.

The NYSSCPA SEC Practice Committee and Technology Assurance Committee deliberated the exposure draft and prepared the attached comments. If you would like additional discussion with the committee, please contact Joel Lanz, chair of the Technology Assurance Committee, at (516) 933-3662, or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,



President

Attachment

**NEW YORK STATE SOCIETY OF
CERTIFIED PUBLIC ACCOUNTANTS**

**COMMENTS ON PROPOSED COSO GUIDANCE FOR SMALLER PUBLIC
COMPANIES REPORTING ON INTERNAL CONTROL OVER FINANCIAL
REPORTING**

January 13, 2006

Principal Drafters

Joel Lanz, Chair, Technology Assurance Committee

Bruce Nearon, Technology Assurance Committee

Anthony Chan, SEC Committee

NYSSCPA 2005 – 2006 Board of Directors

Stephen F. Langowski,
President

Thomas E. Riley,
President-elect

Raymond M. Nowicki,
Secretary

Neville Grusd,
Treasurer

Susan R. Schoenfeld,
Vice President

Stephen P. Valenti
Vice President

Louis Grumet,
ex officio

William Aiken

Deborah L. Bailey-Browne

Thomas P. Casey

Ann B. Cohen

Michelle A. Cohen

Debbie A. Cutler

Anthony G. Duffy

Robert L. Ecker

Mark Ellis

David Evangelista

Joseph M. Falbo, Jr.

Dr. Myrna L. Fischman

Daniel M. Fordham

Phillip E. Goldstein

Raymond P. Jones

John J. Kearney

Don A. Kiamie

John J. Lauchert

Howard B. Lorch

Beatrix G. McKane

David J. Moynihan

Ian M. Nelson

Jason M. Palmer

Richard E. Piluso

Robert T. Quarte

C. Daniel Stubbs, Jr.

Anthony J. Tanzi

Edward J. Torres

Robert N. Waxman

Philip G. Westcott

Ellen L. Williams

Richard Zerah

NYSSCPA 2005 - 2006 Accounting & Auditing Oversight Committee

Paul D. Warner, Chair

George I. Victor, Vice Chair

Elliot L. Hendler

Joel Lanz

Michele M. Levine

Thomas O. Linder

Joseph A. Maffia

Robert S. Manzella

Mitchell J. Mertz

Mark Mycio

Eric J. Rogers

Warren Ruppel

Ira M. Talbi

Elizabeth K. Venuti

Paul J. Wendell

Margaret A. Wood

NYSSCPA 2005 - 2006 SEC Practice Committee

Mitchell J. Mertz, Chair	Edward J. Halas	Joel C. Quall
Eric H. Altstadter	Elliot L. Hendler	Arthur J. Radin
Michele B. Amato	David J. Lamb	Michael E. Rhodes
Patricia A. Baldowski	Gregory J. Lavin	John P. Rushford
John A. Basile	Eric P. Lerner	Paul Rykowski
Bruce Baylson	Elliot A. Lesser	Stephen A. Scarpati
Douglas J. Beck	Moshe S. Levitin	Sunil K. Singla
Michael C. Bernstein	Helen R. Liao	Matthew A. Snyder
Jeffrey M. Brinn	Thomas P. Martin	Robert E. Sohr
Thomas E. Caner	Nicole J. Martucci	Fredric S. Starker
Anthony S. Chan	Corey L. Massella	Mihyang Tenzer
Tony W. Cheng	Jacob Mathews	Joseph Troche
Burgman E. Connolly	Michael A. Naparstek	George I. Victor
Joseph Davi	Walter Orenstein	Philip H. Weiner
Robert Fener	Rita M. Piazza	Paul J. Wendell
Leon J. Gutmann	Peter J. Pirando	David C. Wright

NYSSCPA 2005 - 2006 Technology Assurance Committee

Joel Lanz, Chair	Michael P. Gawley	Joseph B. O'Donnell
Karina Barton	Mudit Gupta	Joy M. Paulsen
Harvey G. Beringer	Joanne M. Knight	Paul Rafanello
Kenneth J. Burstiner	Lucas Kowal	David A. Rauch
Gary E. Carpenter	Richard Lanza	Yigal Rechtman
Mark S. Chapin	Ford J. Levy	Walter C. Schmidt
Frank J. DeCandido	Jennifer A. Moore	Ryan Youngwon Shin
Brian Friedman	Yossef Newman	Bruce I. Sussman
		Irwin Winstein

NYSSCPA Staff

Ernest J. Markezin

**New York State Society of CPAs
Comments to Committee on Sponsoring Organizations (COSO) on
Guidance for Smaller Public Companies Reporting on Internal Control over
Financial Reporting:
Exposure Draft**

January 13, 2006

General Comments

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recognizes in its draft Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting (the draft Guidance) that Section 404 of the Sarbanes-Oxley Act of 2002 is a major driver of public companies' evaluations of internal controls over financial reporting. The draft Guidance reaffirms the appropriateness of concepts and principles first set forth by COSO in 1992. The original COSO framework is based on 26 fundamental principles, which are equally applicable to all organizations, both large and small, according to COSO.

COSO recognizes the need for greater formalization in the control processes and for a certain minimum level of documentation to provide evidence that the internal controls are operating effectively. This level of documentation increases when management makes assertions to third-parties about the effectiveness of an entity's internal controls.

COSO recognizes the need to keep costs associated with internal controls reasonable. It acknowledges several of the differences between smaller and larger businesses, including:

- Actions of management and its demonstrated commitment to effective governance and control (the tone at the top) is often more transparent to employees in smaller organizations.
- Information technology can be used by smaller organizations to facilitate internal controls. For example, controls in off-the-shelf software can be implemented.
- Monitoring by executives who have a direct and explicit knowledge of the activities of the business can be an effective control.

We recognize the truism of many comments in the draft Guidance. For instance, significant reviews of operations by management of smaller organizations increase the potential for management override of internal controls. Adequate segregation of duties may not be possible due to limited resources. Attracting independent board members with financial and operating expertise will be challenging.

Our comments, which follow, recognize the judgment which will be required by smaller organizations. The right tone at the top is critically important. Nevertheless, we are concerned with the need for more reliance on compensating controls, closer management

oversight and the inherent risks it creates, and the need for effective board oversight without the board usurping management’s responsibilities. We also are concerned with the limited guidance in the area of control documentation.

The original *Internal Control – Integrated Framework* was not limited to public companies. This guidance should not be so limited. It should be applicable to all small companies.

We appreciate the opportunity to comment and hope that our comments will be helpful to COSO.

Specific Comments

The following are specific comments on the draft Guidance and follow the order of the captioned topics within the exposure draft:

COSO EXECUTIVE SUMMARY

Controls Need to Be Cost Effective for Small Business

p.4 “Use Information Technology to Standardize Controls – Information technology (accounting software) can be used to (a) implement consistent controls, and (b) enhance segregation of duties.”

Comment: Use of information technology (IT) in small companies often results in significant segregation-of-duty-issues due to lack of sufficient IT human resources and training. In small companies, IT personnel typically have complete control over the network, operating systems, and application software. Furthermore, they can make changes to accounting records to correct errors. This creates improper segregation of duties, rather than enhancing them.

COSO GUIDANCE

1. OVERVIEW

Comment: None

2. SMALLER COMPANY PERSPECTIVES

Challenges in Implementing Internal Control in Smaller Business

Information Technology

p.18 “The level of effort required to establish effective internal control over information technology is largely, although not completely, a reflection of the extent of standard, packaged software versus custom, in-house developed software.

Comment: This is often the refrain of management and auditors who do not fully grasp the effect of IT on internal control. Assuming that little effort to document and assess IT is necessary because standard packaged software is used is an erroneous assumption. It is the rare small company that does not have one or more of the following IT attributes that create risk to financial information:

- A network
- A domain controller
- An e-mail server
- High-speed Internet access
- IT consultants
- IT vendors
- Outsourced IT services
- Firewalls and routers

Small companies may grant all accounting users full access rights to all accounting functions. IT and vendors are often granted full access rights to all information assets. To compound the problem, vendors and consultants are often granted remote access rights to company networks without any monitoring.

p.18 “Fewer controls over change management are needed when companies use standard, highly-regarded accounting packages that do not allow users to modify programs than when companies rely on in-house software under the direct control of only a few individuals.”

Even the most basic accounting packages have a multitude of configuration options available. Small companies rarely document the options they implement; often abdicating implementation to consultants and vendors who likewise do not document the features they enable. Although small companies do not need to have elaborate System Development Life Cycle (SDLC) standards, they do need to have at least some level of policies and procedures such as authorization and documentation of accounting package purchase decisions, implementation, and testing. None of this, however, negates the need for documenting and assessing operating system and network operation and access security controls.

3. CONTROL ENVIRONMENT

Importance of Board of Directors

Basic Principle

p.29. “The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.”

Comment: Effective use of IT is an integral part of internal control. In fact, all of the five top-level components of internal control, as well as many manual controls, rely on IT. Furthermore, IT is the enabler and repository of the documentation that evidences management’s compliance with the Sarbanes Oxley Act.

p.29 “*Financial Expertise* – The board of directors and audit committee have one or more members who have financial expertise.”

Comment: Due to the importance and pervasiveness of IT, the Board should also include one or more members who understand IT and related controls.

Approaches Smaller Companies Can Take to Achieve the Principle

Examples of Effective Ways to Achieve the Principle

p.32 “**Audit Committee Considering Management Override of Controls.**

The audit committee discusses, in executive session at least annually, its assessment of the risks of management override of internal control, including discussion of why management might override controls and how it would conceal its activities.”

Comment: See The Panel on Audit Effectiveness report, also known as the O’Malley Report, which found that IT is often used to facilitate management’s override of controls. The audit committee should also discuss how IT can be used to override controls and conceal such activity.

p.32 “Audit committee members occasionally make inquiries of members of management not responsible for financial reporting (such as sales managers, procurement managers, human resource managers, and so forth) to seek information about any possible concerns about ethics and any management override of internal controls.”

Comment: Audit committees should inquire with IT managers about whether they have been asked to override controls by management and the risk of using IT to override controls.

p.33 “**Audit Committee Setting Meeting Contents.**

The audit committee establishes of calendar of topics for review...”

Comment: The Other Members of Management section should include the IT Manager who should report on the following:

- a. Security incident activity
- b. Status of IT control deficiencies, noted by the auditors and remediation status
- c. IT budget, if material
- d. Long-term IT strategy

4. RISK ASSESSMENT

p.48 “The output of the risk assessment process is important to the design and operation...”

Comment: The risk assessment process also helps management justify remedial action that will be taken, rather than simply identifying controls that should be implemented.

p.49 “Errors, irregularities and misstatements might include:...”

Comment: COSO should also consider incorrect standing or operational data on which financial reporting activity may take place (e.g., a computer generated report that improperly identifies past due receivables).

p.50 “**Risk Assessment Principles**”

Comment: Although the risk assessment requirements of SAS 99 are included here, those required by SAS 94 (impact of IT), which are specifically required in planning and determining financial audit risk, are not but should be.

p.51 “*A precondition to risk assessment is the establishment of objectives for reliable financial reporting.*”

Comment: If the Financial Statement Assertions identified on the page rely on IT (completeness, allocation), the impact of IT should be considered, and the reliability of the system should also be determined using a framework such as the SysTrust principles.

p.52 “management identifies processes supporting these financial statement accounts.”

Comment: Computerized processes should be considered here.

p.53 “**Risk Assessment Overview Diagram**”

Comment: The underlying impact of IT on financial activities should be reflected in risk assessment, rather than later as a control activity. Properly assessing and managing technology risk can then have specific impacts on control activities.

Identification and Analysis of Financial Reporting Risks

Approaches Smaller Companies Can Take to Achieve the Principle

p.54 “Identifying and mapping IT systems”

Comment: Given the evolution of networks, mapping should also include which networks are impacted. Control over the network permits control over the server, which then permits control of the application.

p. 57 “**Analyzing Risk for Information Technology**”

Comment: The example given illustrates a number of common misunderstandings related to the impact and role of IT on the financial audit.

- The focus is on critical applications, but the underlying network risks and controls that can circumvent application controls are not mentioned.
- IT should be part of the risk assessment, not something considered after the fact. A list of critical resources should be considered during the risk assessment in order to comply with SAS 94 and to educate the business user about the behind-the-scenes risks.
- Web applications do not necessarily reduce the risk or number of processes. Due to the high risk of payment applications on the Internet, organizations such as the Payment Card Industry (e.g., Visa and MasterCard) have issued significant guidelines and requirements.
- The impact of network exposures should be appropriately considered as well as their impact on applications.

5. CONTROL ACTIVITIES

p.74 “**Control Activities for Outsourcing Activities Where a SAS 70 Report Is Available**”

Comment: Since SysTrust would provide better assurance for outsourced activities, it should be mentioned as an example of a third party report, rather than just SAS 70.

p.81. “*General Computer Controls* – General computer controls are broad and include controls over access, change and incident management, systems development and deployment, data backup and recovery, third party vendor management, and physical security critical to the integrity of the financial reporting process.”

Comment: According to COSO (1992), general controls include:

- Data Center
- Operating system development and maintenance
- Application software acquisition, development, implementation, and maintenance
- Access security.

There are still data centers at small companies called server rooms. Before there was wide-spread diffusion of IT to small companies, the auditor’s evaluation of controls in the data center included an assessment of data center management. Small companies typically have IT management and at least one or more employees and consultants. IT management in small companies needs to be evaluated to comply with COSO (1992).

p.86 “[Passwords] Are at least six alphanumeric characters”

Comment: In today’s environment, six characters are insufficient and can quickly be cracked by hackers. Even Microsoft recommends a minimum of seven.

p.86 “[Passwords] Are remembered and cannot be reused for five changes.”

Comment: Five old passwords are insufficient because it defeats the control of forcing users to change passwords. It should be at least 12, and needs to be coupled with a minimum password age of one day.

6. MONITORING

p.107 “By appending monitoring of controls into routine monitoring of operations, management can integrate monitoring of internal control at lesser cost.”

Comment: “Appending” contradicts the theory of integrated internal controls and its corollary that building controls into a process (integrating) is less costly and more effective than tacking them on after the fact.

Other Comments

1. Set the right tone and encourage early implementation.

COSO is to be commended for acknowledging the challenges faced by smaller public companies while confirming the need for implementing cost-effective controls. Although extra time has been given to smaller public companies to comply with the Sarbanes 404 provisions, most of them have not taken advantage of the time extension to evaluate and enhance their internal controls. To help generate a stronger interest in early assessment of internal controls, COSO should use this opportunity to articulate the benefits of early controls assessment and Sarbanes Oxley implementation.

2. The concept of “building controls into the culture” should be expanded.

Building controls into the culture is critical to maintaining a strong control environment, and improving controls on a continuous basis. Until now, there has been no official guidance promoting the benefit of building controls into the culture, thereby strengthening the foundation of the company’s internal control structure. To solidify users’ understanding of this concept, COSO should reaffirm that:

- a. Control improvement is not a one-time event.
- b. Control failures are avoidable when companies take an active role in monitoring and strengthening the integrity of their control activities.
- c. Cost-effectiveness implementation is a direct result of early planning, in-depth assessment of the related risks, and early identification and remediation of control gaps.

3. Guidance on “Formalization of Controls and Documentation” should be expanded.

Identifying the relevant controls and formalizing the manner with which the related

activities should be evidenced are two key aspects of the Sarbanes 404 compliance process. Most public companies that implemented Sarbanes 404 in year one struggled with maintaining the right combination of preventive and detective controls and the right level of control documentation. Given the extent of judgment and internal control expertise required, best practices and other relevant examples should be included to illustrate what key control activities (by business cycle or process) should be performed and how they should be documented.

COSO's limited guidance on the formalization and documentation of controls is of concern. COSO recognizes that smaller companies "...may implement effective internal controls in a different manner" and that controls may be less formal because of management's hands-on approach. Yet COSO points out that: "When management asserts to a third party on the design and operating effectiveness of internal control, there usually is a need for greater formalization in the control processes and a certain level of documentation to provide evidence the controls are working effectively." This is an area that requires more direction in COSO's Guidance. Otherwise, it will become a contentious issue as auditors attempt to opine on companies' 404 assertions.

Judgment will be required to effectively adopt the COSO principles at smaller companies. This may result in reliance on less formalized control procedures or in a different level of control documentation than observed at larger registrants. Although not an issue for COSO directly, we are concerned that regulators (such as the PCAOB or the SEC) may, with hindsight, expect a more formalized approach to either implementation of controls or documentation surrounding the control environment.

4. Discuss the need to involve the right talents upfront.

Although the draft Guidance has methodically described the process of implementing the COSO framework, it alone does not result in a cost-effective Sarbanes 404 implementation. COSO should explain the expertise and knowledge required to comply with the Sarbanes 404 provisions effectively and efficiently. Specifically, COSO should encourage smaller public companies to involve the appropriate internal and external resources right from the start.

5. Not all 26 principles are equally important.

Effective internal control does not mean that users must meet all 26 principles as outlined in the draft Guidance. As highlighted in Exhibit 2.3 of the draft Guidance, users should be advised to put additional emphasis on the integrity of their control environment and monitoring control procedures as they apply this internal control framework. The key is to customize controls to mitigate the relevant fraud and financial reporting risks.

6. The role of technology should be clarified.

Technology is only a means to an end and can be an effective tool to help enhance internal control. Prior to applying any technology-based solution, users must first assess the relevant risks, identify the related control gaps, and develop the relevant

control activities to mitigate them.

7. **The suggested templates and evaluation matrix are for reference purposes only.** COSO's templates and evaluation matrix should not be taken "as is." COSO should advise users of the need to customize controls to mitigate the relevant risks, and remind them of the nature and purpose of this draft Guidance.