new york state society of
NYSSCPA
certified public accountants

Home of the Trusted Professional
3 park avenue, at 34th street, new york, ny 10016-5991
212.719.8300 • fax 212.719.3364
www.nysscpa.org

July 5, 2006

Mr. Thomas Lamm
Director of Research, Staff Liaison - Standards Board
Information Systems Audit and Control Association
3701 Algonquin Road
Suite 1010
Rolling Meadows, Illinois 60008

By e-mail: research@isaca.org

Re: Proposed IT Control Objectives for Sarbanes Oxley – 2nd Edition

Dear Mr. Lamm:

The New York State Society of Certified Public Accountants, the oldest state accounting association, representing approximately 30,000 CPAs, welcomes the opportunity to comment on the Proposed Information System Auditing Procedure referenced above.

The NYSSCPA Technology Assurance Committee deliberated the exposure draft and has prepared the attached comments. If you would like additional discussion with the committee, please contact Yigal Rechtman, member of the Technology Assurance Committee, at (212) 684-0011, or Ernest J. Markezin of the NYSSCPA staff, at (212) 719-8303.

Sincerely,

Thomas E. Riley
President

Attachment

NEW YORK STATE SOCIETY OF

CERTIFIED PUBLIC ACCOUNTANTS

COMMENTS TO THE INFORMATION SECURITY AUDIT AND CONTROL ASSOCIATION (ISACA) ON INFORMATION TECHNOLOGY (IT) CONTROL OBJECTIVES FOR SARBANES OXLEY – 2ND EDITION

July 5, 2006

Principal Drafters

Yigal Rechtman
Bruce Sussman
Joseph B. O'Donnell

NYSSCPA 2006 – 2007 Board of Directors

Thomas E. Riley, *President*
David A. Lifson, *President-elect*
Mark Ellis, *Secretary*
Neville Grusd, *Treasurer*
Sharon S. Fierstein, *Vice President*
Richard E. Piluso, *Vice President*
Robert E. Sohr, *Vice President*
Louis Grumet, *ex officio*
Edward L. Arcara
Deborah L. Bailey-Browne
Kathleen G. Brown
Thomas P. Casey
Debbie A. Cutler
Anthony G. Duffy
David Evangelista
Joseph M. Falbo, Jr.
Myrna L. Fischman, PhD.
Daniel M. Fordham
Phillip E. Goldstein
Scott Hotalen
Don A. Kiamie
Lauren L. Kincaid
Stephen F. Langowski
John J. Lauchert
Kevin Leifer
Elliot A. Lesser
Howard B. Lorch
Beatrix G. McKane
Mark L. Meinberg
Ian M. Nelson
Jason M. Palmer
Robert A. Pryba Jr.
Robert T. Quarte
Judith I. Seidman
C. Daniel Stubbs, Jr.
Anthony J. Tanzi
Edward J. Torres
Liren Wei
Ellen L. Williams
Margaret A. Wood
Richard Zerah

NYSSCPA 2006 - 2007 Accounting & Auditing Oversight Committee

George I. Victor, Chair
Robert W. Berliner
Elliot L. Hendler
Joel Lanz
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 2006 - 2007 Technology Assurance Committee

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

NYSSCPA Staff

Ernest J. Markezin

New York State Society of CPAs

Comments to the Information Security Audit and Control Association (ISACA) on Information Technology (IT) Control Objectives for Sarbanes Oxley – 2nd edition

General Comments

The Exposure Draft (ED) of April 30, 2006 continues a well thought out framework that discusses the effect of the Sarbanes-Oxley Act of 2002 (the Act) on financial statement auditors considering the integration of Information Technology in their procedures. The updated ED includes important additions and is timely in its feedback feature in appendixes such as "Lessons Learned" and illustrative procedures addressing the Act's objectives and requirements.

Overall, we consider the ED to be a well formed and relevant guide to the professional practice of IT audit and security. The ED is framed as ISACA guidance, which is lower in authority than a standard. We wish to offer additional commentary on items which are well focused, as well as on those requiring some degree of further analysis or development.

Specific Comments

Well focused Items:

The ED serves its users well by establishing the relationship between risk-based audits and the complexity of IT in organizations of varying sizes. The distinction between enterprise resource planning (ERP) and simpler accounting IT platforms is a good example of such variation in complexity. The underlying risk-based approach is well established and properly incorporated in the ED.

Items which require further thought:

1. The issue of prioritization of controls may lead to a problematic interpretation. While it may be a practical approach, prioritizing controls could short-circuit the intentions of the ED's authors. Identifying key controls contradicts the risk-based approach that is so well defined throughout the ED. When identifying key-controls, there is the adverse possibility that IT specialists and/or auditors – not well versed in each other's area – will use the "flagged" key controls without critically thinking of the risk-based selection of controls. For example, if a control was pre-selected under this ED as a "key control", there is a possibility that an auditor not familiar with the applicability of such control to a particular organization under audit may automatically identify it as a "key" control. Other areas, which might otherwise be identified in a risk

based approach, may be overlooked in a prioritization approach because of a preconception of a lower prioritization. **Our recommendation** is to remove the reference to prioritized controls from the body of the ED, and to strongly qualify usage of this concept as illustrative.

2. The ED incorporates an appendix that addresses the approach to spreadsheets. The ED authors correctly identify this issue as a possible control risk. However, the risk should be further generalized to all forms of end-user computing, both by generalized software such as spreadsheets, through end-user special applications to mal-ware that is not controlled by the end-user and nonetheless poses a control risk to the organization.

   Our recommendation is to expand the discussion of the risks embedded in end-user computing. Such a discussion should at minimum encompass:

   - The age of the application and the circumstances under which it was acquired.

   - Whether the application was purchased off the shelf, or alternatively, was customized. Should the enterprise use a customized application, the auditor should consider whether there is evidence supporting the application of the enterprise's system development methodology.

   - If the application has been customized, the auditor should inquire by whom. If it becomes evident that the application was installed or maintained by outsourced vendors or contractors, the auditor should consider whether the enterprise has effective vendor management controls which address quality assurance and integrity and security considerations.

3. We agree with the inclusion of a new section which addresses the human element of implementing and maintaining a Sarbanes program. This is a very positive step which should be enhanced by reminding the auditor to consider the overall "tone at the top" of the organization. Since the standard refers to The Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control framework, it would only be logical to remind auditors that the control culture is directly linked to the tone established by management. We would also suggest that the standard remind the CPA to consider the existence of a company ethics program. Within the control environment, the CPA should also consider whether management links overall compliance to its performance management and compensation program.

4. Selecting sample sizes is a significant issue for organizations and their auditors. Figure 7 on page 39 of the ED provides sample size selection based on what the ED terms a "common (minimum) sample size selection." The origin of these recommended sample sizes is not stated. For instance, are these sample sizes based on the opinion of a group of experts and/or the practices of

a number of large audit firms? The ED does not indicate whether these sample sizes have a theoretical basis, such as statistical sampling. Also, the ED is silent on how the sample sizes relate to levels of confidence and whether sample sizes are influenced by levels of risk assessment. In addition, the ED does not address associated tolerance levels for internal control testing exceptions. For example, if one exception is identified, should the control be considered deficient?

Our recommendation is to include the origin of the recommended sample sizes and provide the theoretical basis (if any) for these sample sizes, as well as provide recommend exception tolerance levels for the different sample sizes and discussion of confidence levels and risk assessment levels on sample size selection.

5. The Lessons Learned (Figure 44) portion of the document is a very useful addition to this version of ED. **Our recommendation** is that the importance of the "Lessons Learned" be emphasized by providing references to them in the related parts of the main document. For example, in the Plan and Scope section (page 34) should make reference to Lessons Learned - Plan and Scope that is provided in Figure 44. Also, the origin of the lessons learned should be provided. If these are experiences of the organizations of the ED authors then this should be stated in the ED. In the case where the lesson learned is described in greater detail in a published document or web site, we recommend that reference to this document be included in the ED. This would allow individuals in companies and auditors of these companies to have a greater understanding of problems to avoid in complying with Sarbanes-Oxley regulations.

6. The ED discusses the challenges facing smaller companies in complying with regulations such as the Sarbanes-Oxley Act in numerous sections throughout the document. The importance of this issue is evidenced by regulatory and advisory organizations' plans to issue separate guidance on this issue. COSO released an exposure draft in November 2005 (as stated in the ED) entitled "Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting." In addition, the Public Company Accounting Oversight Board (PCAOB) plans to develop or facilitate the development of implementation guidance for the auditor of smaller companies[1]. Accordingly, the IT Governance Committee should consider providing a more comprehensive discussion of smaller company regulation compliance issues and recommended implementation strategies to address these issues.

Our recommendation is expanded discussion of smaller company regulation issues and strategies for the near future in a separate section of the ED that is entirely devoted to this topic. We recommend that, at the very least, an

[1] PCAOB May 17, 2006 press release located at
http://www.pcaobus.org/News_and_Events/News/2006/05-17.aspx

appendix be created to summarize the most significant issues and strategies to address smaller company issues. This would provide much needed guidance to smaller companies and their auditors in controlling compliance costs. In the long term, we recommend that the IT Governance Institute consider issuing separate guidance for smaller companies' IT Control Objective for Sarbanes-Oxley.