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

February 9, 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 Information System Auditing Procedure on Business Application Change Control

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,

Stephen F. Langowski

Stephen F. Langowski
President

Attachment

NEW YORK STATE SOCIETY OF

CERTIFIED PUBLIC ACCOUNTANTS

Comments to the Information Security Audit and Control Association (ISACA) on Standards Documents Under Exposure: BUSINESS APPLICATION CHANGE CONTROL

February 9, 2006

Principal Drafters

Yigal Rechtman
Joel Lanz

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
Kathleen G. Brown
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.
Myrna L. Fischman, PhD.
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
Victor S. Rich
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 Technology Assurance Committee

Joel Lanz, Chair
Karina Barton
Harvey G. Beringer
Kenneth J. Burstiner
Gary E. Carpenter
Mark S. Chapin
Frank J. DeCandido
Brian Friedman
Michael P. Gawley
Mudit Gupta
Joanne M. Knight
Lucas Kowal
Richard Lanza
Ford J. Levy
Jennifer A. Moore
Yossef Newman
Joseph B. O'Donnell
Joy M. Paulsen
Paul Rafanello
David A. Rauch
Yigal Rechtman
Walter C. Schmidt
Ryan Youngwon Shin
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 Standards Documents Under Exposure:
Business Application Change Control
February 9, 2006

Specific Comments
Specific comments on the exposure draft are as follows, listed by section number as presented in this ISACA exposure draft:

1.3.3 ISACA's exposure draft (ED) defines primary and secondary controls to a system development life cycle (SDLC). "Efficiency and Effectiveness" are placed as primary goals and "Reliability" is placed as a secondary goal. These placements should be reversed in order that "Reliability" is a primary goal of the SDLC and "Efficiency and Effectiveness" are a secondary goal. The reasoning for such ordering is that the outcome of the SDLC process should be a reliable control. Efficient SDLC, while desired, occurs only when a change occurs. Reliability should be the prime objective.

2.1.2 The internal audit department (IAD) is guided to assess various factors in its planning of the SDLC. Among the factors the ED enumerates is a check that "Budgetary estimates are realized". The issue of budgetary adherence is important in terms of assessing risks, but not in terms of a primary goal of the SDLC. The budgetary tool is only an aid for planning and feedback on actual results in SDLC.

4.2.3 This section states that "IT [the IT department] must use a tracking system …" The statement is in contrast to two facets of the guidance of the ED. First, the ED as defined, is designed to guide the IS auditor, not the management of the IT department. Second, the word "must" is inappropriate as it describes a requirement. The guide is not designed to set requirements, but to aid the IS auditor to properly assess risks and apply requirements as they are described by standards. Accordingly, this section should be re-worded.

4.4.2 This section addresses a "true validation/confirmation" of the testing. A literal definition of "true" is absolute. However, IS audits in general are risk-based, in which case absolute validation cannot be attained. Accordingly, this sentence should be revised to address a "reasonable validation or confirmation".

4.4.3 The section concludes with a note "this control should not be relied upon to detect fraud". It is not entirely clear what purpose the note is meant to serve in relation to the section. This note should be revised or expanded to properly address the objectives of the guide under exposure and better relate to the section.

4.5.1 The section concludes with “Finally, malicious programs can be introduced…” This is an example for one type of risk (malicious programs) but not a description of the risk-prone activity as a whole. This wording should be revised to a more general nature of describing the risks of change implementation.

5.1.1 This section describes emergency change process. The section details the time frame of 24 hours to prevent or avoid recurrence of any significant outage. This guidance is somewhat arbitrary as some applications may be able to sustain only a few minutes of outage while others may be able to sustain much more than 24 hours. The required duration in terms of time elapsed is clearly stated in section 5.1.2 as “a required period of time based on the business and legislative risk of the change”.

5.1.2 This section describes emergency changes. Certain steps are specifically described and others more generally. A “post mortem with root cause analysis” may be a technical jargon term that should be either defined or expanded upon. It is not evident from the guide under exposure what this term entails.

5.4.1 The word “should” states a requirement for the IS auditor. The term should be revised to a risk-based action such as “may, based on assessed risk”.

5.5 The section addresses preventive control. However, the section is in conflict with section 5.7. Section 5.5 describes steps the IS auditor should take while the latter section describes steps to be taken by management. Based on the intended audience for this guide, section 5.7 should clarify its position in terms of SDLC and the IS auditor, not management.

7.2.1 The section states “there should be agreement on the type of change control testing…” The section is not clear about the agreeing parties, the timing of the agreement in the SDLC and other issues related to testing of change control that should be considered.