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 11, 2009

Mr. J. Gordon Seymour
Office of the Secretary
PCAOB
1666 K Street, N.W.
Washington, DC 20006-2803

By e-mail: comments@pcaobus.org

Re: PCAOB Release 2008-006: Proposed Auditing Standards Related to the Auditor's Assessment of and Response to Risk; Proposed Conforming Amendments to PCAOB Standards (Rulemaking Docket Matter No. 026)

Comments on Proposed Auditing Standard – *The Auditor's Responses to the Risks of Material Misstatement*

Dear Mr. Seymour:

The New York State Society of Certified Public Accountants, representing 30,000 CPAs in public practice, industry, government and education, submits the following comments to you regarding the above captioned exposure draft. The NYSSCPA thanks the PCAOB for the opportunity to comment.

The NYSSCPA's Technology Assurance Committee deliberated the exposure draft, in particular Appendix 4, Proposed Auditing Standard – *The Auditor's Responses to the Risks of Material Misstatement*, page A4–13–37, and drafted the attached comments. If you would like additional discussion with us, please contact Bruce I. Sussman, Chair of the Technology Assurance Committee, at (973) 422-7151, or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,

Sharon Sabba Fierstein

Sharon Sabba Fierstein
President

Attachment

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

COMMENTS ON APPENDIX 4, PROPOSED AUDITING STANDARD – *THE AUDITOR'S RESPONSES TO THE RISKS OF MATERIAL MISSTATEMENT*, PAGE A4–13–37, OF PCAOB RELEASE 2008-006: PROPOSED AUDITING STANDARDS RELATED TO THE AUDITOR'S ASSESSMENT OF AND RESPONSE TO RISK (RULEMAKING DOCKET MATTER NO. 026)

February 11, 2009

Principal Drafters

Michael A. Pinna
Yigal Rechtman
Bruce I. Sussman

NYSSCPA 2008–2009 Board of Directors

Sharon Sabba Fierstein, *President*
David J. Moynihan, *President-elect*
Richard E. Piluso, *Secretary/Treasurer*
Barbara S. Dwyer, *Vice President*
Joseph M. Falbo Jr., *Vice President*
Elliot L. Hendler, *Vice President*
Margaret A. Wood, *Vice President*
Louis Grumet, *ex officio*
Scott M. Adair
Edward L. Arcara
John Barone
Susan M. Barossi
S. David Belsky
Thomas Boyd
Anthony Cassella
Cynthia D. Finn
Robert L. Goecks
David R. Herman
Scott Hotalen
John B. Huttlinger, Jr.
Martha A. Jaeckle
Suzanne M. Jensen
Lauren L. Kincaid
Gail M. Kinsella
Nancy A. Kirby
J. Michael Kirkland
Kevin Leifer
Elliot A. Lesser
David A. Lifson
Anthony J. Maltese
Mark L. Meinberg
Avery E. Neumark
Robert A. Pryba, Jr.
Joel C. Quall
Ita M. Rahilly
Judith I. Seidman
Thomas M. VanHatten
Liren Wei
Charles J. Weintraub

NYSSCPA 2008 - 2009 Accounting & Auditing Oversight Committee

Mitchell J. Mertz, *Chair*
Michael J. Aroyo
Robert W. Berliner
Edward P. Ichart
Thomas O. Linder
Rita M. Piazza
William M. Stocker III
Bruce I. Sussman
Ira M. Talbi
George I. Victor
Robert N. Waxman

NYSSCPA 2008–2009 Technology Assurance Committee

Bruce I. Sussman, *Chair*
Harvey G. Beringer
Gary E. Carpenter
Matthew Clohessy
David O. Daniels
Adam Dunning
Matthew Giordano
Mudit Gupta
Patrick Helmes
Lucas Kowal
Joel Lanz
Richard Lanza
Yosef Levine
Jennifer A. Moore
Bruce H. Nearon
Yossef Newman
Joseph B. O'Donnell
Karina Pinch
Michael Pinch
Michael A. Pinna
Yigal Rechtman
Robyn Sachs
Walter Schmidt
Sheryl Skolnik
Inga Sokolova
Irwin Winsten

NYSSCPA Staff

Ernest J. Markezin
William R. Lalli

New York State Society of Certified Public Accountants

Comments on Appendix 4, Proposed Auditing Standard – *The Auditor's Responses to The Risks Of Material Misstatement,* Page A4–13–37, Of Proposed PCAOB Release 2008-006: Proposed Auditing Standards Related To The Auditor's Assessment Of And Response To Risk

The Society's Technology Assurance Committee deliberated page A4–13–37 of the proposed standard and has prepared the following comments. We wish to thank the PCAOB for the opportunity to comment.

Response Summary

The concept of benchmarking is one in which a baseline performance level for automated controls is established and then, in future years, auditors might not need to retest the effectiveness of that automated control in order to rely on it. However, reliance on the effectiveness of automated controls should not be based on the results of a previous audit. We believe that in today's complex information system environments, it is inappropriate to rely on benchmarking in an audit for the reasons discussed below. In addition, in circumstances where the auditor deems the information technology (IT) environment to be a significant internal control component, the environment should be tested every period. We believe that regular testing eliminates the need to use benchmarking as a control evaluation method.

Introduction

The automation of internal controls has become a substantial portion of the operations of companies large and small alike. Systems previously referred to as "Electronic Data Processing" (EDP) were serial in nature and simplistic in operation. Over decades, EDP systems have evolved into multi-platform, complex IT environments. Modern IT environments require auditors to obtain a thorough understanding and to perform a detailed analysis of EDP in order to be assured that such a system is well suited for the function it serves and that it operates as designed.

Discussion

Currently, automated controls are implemented by way of IT utilizing software, hardware, operating systems and "middle-ware." IT is a complex, multi-dimensional environment that no longer can be considered a simple "input-process-output" paradigm. Substantial detailed consideration and analysis need to be integrated within the attest procedures that assess the risks and operational effectiveness of an IT environment.

Benchmarking is generally the weakest strategy of the available alternatives for the evaluation of automated controls. Benchmarking is ineffective in many situations because most automated controls applications are key controls in the overall internal control environment. These key controls are often implemented as complex, multi-layered software or hardware applications. Such complex software is multi-modular and

many factors affect the method by which the software receives, processes, stores, and outputs the information.

Automated controls that are implemented as complex software involve a large number of variables. Accordingly, each of these variables can affect the reliability of the control. The susceptibility of a control to ineffectiveness increases exponentially with the number of variables that are involved in its operations. The possibility exists that the passage of time may reveal that software which has been previously evaluated to be stable and reliable might contain variables and values unforeseen by the software designers and implementers that could adversely affect its reliability. For example:

a. In the late 1990s, many software vendors needed to re-write software code in order to accommodate a potential high-risk situation in which software would have treated the year 2000 as the year 1900. This scenario, known as "Y2K," could have affected controls that were previously effective in complex software environments. Therefore, the automated control that had been used for several decades could not withstand a certain set of values due to an unforeseen design limitation.
b. Automated software controls designed to calculate interest rates rounded to six decimal places used a memory format that allowed it to operate properly with interest rates that did not exceed 10%. However, when interest rates exceeded this limit, the same software that had been considered "mature and stable," failed to operate as designed.
c. Automated controls that were implemented assuming that three decimal places of accuracy were sufficient might not operate effectively when large market fluctuations require iterative calculations where a very large dollar amount is multiplied by a very small percentage. Because automated controls ultimately operate in a limited-memory universe, very precise floating point applications might fail when a combination of variables presents itself, leading to previously unanticipated errors.

In these examples, the effectiveness of the automated controls could vary based on arbitrary conditions which, without testing, would go undetected. In such circumstances, the automated controls would need to undergo and pass a change-management review, including appropriate testing. Reliance on previous results would lend a false sense of security and further steps would need to be taken in order to satisfy the audit requirements for establishing reliance on controls through testing.

Automated controls are closely linked to software implementation. Software design is not implemented in a vacuum; it must take into account the hardware, operating system and middle-ware that underlie the operation of the algorithm. Changes to the operating system, shared libraries from which the software applies certain common functions, drivers, and hardware can all affect the reliability of the software without advance warning. These unintended consequences occur because there is an inherit risk in the design of complex software systems. That risk is based on the method by which software is developed, i.e., the construct of operations. Machine language is abstracted

into programming languages; programming languages are abstracted to programming libraries of re-useable code and libraries of code and abstract algorithms are used as high level tools to create complex software systems. Due to this level of abstraction, an inherit assumption exists for each level's code developer that the underlying levels would operate as designed. In fact, many times underlying levels, such as operating systems or shared libraries, do not operate as designed and seemingly innocent upgrades or updates might affect the reliability of the software adversely.

The concept of applying a benchmarking method to a control solely because it is believed to be "automated" gives rise to several concerns. Auditors would find it difficult to conclude that a modern IT environment which is automated to such a degree can be relied upon without testing. Further, applying a benchmarking method to a manual control would not comply with current audit standards. Accordingly, to propose allowing application of a benchmarking method of an automated control might be viewed as a contradiction of the applicable attest standards.

Benchmarking is an evaluation method that is most suitable to simple control environments in which serial operations are present. Such environments rarely persist because linear processing (input-process-output) is infrequently found in today's business environment. This linear processing has been replaced by control environments that are linked to complex IT environments. The marketplace expects that audit engagements will be able to address such complexities that include ever changing input definitions, processing parameters, and other factors. To that end, we believe that reliance on an automated control for which a low control risk had been assessed previously might result in the occurrence of a material misstatement and that the method might not satisfy external reviews or legal thresholds.

Conclusion

The standards should indicate that reliance on automated controls should be based on testing similar to that which is applied to non-automated controls. Reliance should not be placed on results from previous periods' testing without other testing being performed by the auditor.