



*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

November 7, 2005

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](mailto:research@isaca.org)

**Re: Proposed Information System Auditing Standard on Audit Evidence**

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 Standard 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 Joel Lanz, chair of the Technology Assurance Committee, at (516) 933-3662, committee member Yigal Rechtman, at (212) 684-0011, or Ernest J. Markezin of the NYSSCPA staff, at (212) 719-8303.

Sincerely,

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:  
*AUDIT EVIDENCE***

**November 7, 2005**

**Principal Drafters**

**Yigal Rechtman  
Joseph B. O'Donnell, Ph.D.  
Joy M. Paulsen**

## **NYSSCPA 2005 – 2006 Board of Directors**

Stephen F. Langowski, <i>President</i>	William Aiken	Don A. Kiamie
Thomas E. Riley, <i>President-elect</i>	Deborah L. Bailey-Browne	John J. Lauchert
Raymond M. Nowicki, <i>Secretary</i>	Thomas P. Casey	Howard B. Lorch
Neville Grusd, <i>Treasurer</i>	Ann B. Cohen	Beatrix G. McKane
Susan R. Schoenfeld, <i>Vice President</i>	Michelle A. Cohen	David J. Moynihan
Stephen P. Valenti <i>Vice President</i>	Debbie A. Cutler	Ian M. Nelson
Louis Grumet, <i>ex officio</i>	Anthony G. Duffy	Jason M. Palmer
	Robert L. Ecker	Richard E. Piluso
	Mark Ellis	Robert T. Quarte
	David Evangelista	C. Daniel Stubbs, Jr.
	Joseph M. Falbo, Jr.	Anthony J. Tanzi
	Dr. Myrna L. Fischman	Edward J. Torres
	Daniel M. Fordham	Robert N. Waxman
	Phillip E. Goldstein	Philip G. Westcott
	Raymond P. Jones	Ellen L. Williams
	John J. Kearney	Richard Zerah

### **NYSSCPA 2005 - 2006 Accounting & Auditing Oversight Committee**

Paul D. Warner, Chair	Joseph A. Maffia	Warren Ruppel
George I. Victor, Vice Chair	Robert S. Manzella	Ira M. Talbi
Elliot L. Hendler	Mitchell J. Mertz	Elizabeth K. Venuti
Joel Lanz	Mark Mycio	Paul J. Wendell
Michele M. Levine	Eric J. Rogers	Margaret A. Wood
Thomas O. Linder		

### **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 Information Security Audit and Control Association (ISACA) on  
Standards Documents Under Exposure:  
Audit Evidence**

**November 7, 2005**

**General Comments**

*Applicability of ISACA Proposed Standards*

The scope of the proposed standard overlaps significantly with United States generally accepted auditing standards for financial statement auditing (U.S. GAAS). The problem with this approach is that an information system (IS) audit is not a financial statement audit. Standards for IS audits should focus on IS related activities rather than on the broader responsibilities in a financial statement audit; the proposed standard places general, organization-wide responsibility on the IS auditor rather than focused responsibility on IS. Reference to existing U.S. GAAS requirements should be made (see our specific comment #1, below with respect to U.S. GAAS standard AU. 326 “Evidential Matter”).

Where U.S. GAAS exists, ISACA’s standards should be consistent with them. Not aligning such standards could have the effect of creating confusion in the minds of financial auditors, security experts and the public.

In addition, because ISACA represents an international membership, definitions and standards promulgated by IFAC may be a more acceptable alternative to U.S. GAAS in helping to minimize misunderstandings as to the level of assurance provided under the proposed ISACA standard.

*Use of Terms*

As previously communicated in our response to various ISACA exposure drafts on December 31, 2004, we again express our concern regarding ISACA’s use of terms such as “audit,” “review,” “assurance,” etc., which are well-defined and accepted in the accounting profession’s authoritative literature. The words “audit” and “review” also have legal implications. The proposal does not adequately address the differences in the meaning of similar terms and in the performance expectations between IS engagements by internal auditors and by external auditors (see our specific comment #2 with respect to terminology).

## Specific Comments

The following are specific comments in response to the questionnaire contained in the exposure draft:

1. To what level do you think this is a relevant topic that should be addressed?
  - a. For Certified Public Accountants in the United States, the topic of audit evidence and other attestation standards are covered under Generally Accepted Auditing Standards (GAAS). Generally, when conflict or modifications between GAAS and ISACA standards are present, they should be resolved by referring to GAAS, which are regulated and referred to by CPAs in the United States as the ultimate standards in attestation. Specifically, “Evidential Matter” (AU.326 and AU.9326) provides extensive requirements to CPAs with respect to audit evidence.

Auditors who perform audit procedures which incorporate, include or involve information technologies, will be faced with a challenge with the introduction of the ISACA “Audit Evidence” standard; there may be a perception of two sets of standards that are applicable. Further challenges arise when a CPA is also a member of ISACA and is bound by the two sets of standards that may not be compatible.

As indicated above, CPAs licensed in the USA should adhere to GAAS as their standard for attestation.

2. As presented, do you think this topic is generally accepted to a sufficient level to be adopted by the profession?
  - a. As discussed in our comments below, the proposed standard is not thoroughly evaluated. For example, the terms “audit results” and “audit conclusions” are used interchangeably. Under GAAS these terms are not the same: audit results are the results of audit procedures, as documented by the auditors by means of an opinion letter; audit conclusions are the opinion the auditor expresses in their opinion letter.
  - b. We concur with the exposure draft (ED) when it identifies IS Auditing Standard “Audit Evidence” as a potential new standard for IT auditors. Although the term ‘Evidence’ is defined in S6 Performance of Audit Work, the very nature of audit evidence and it's impact on the outcome of the audit clearly warrants the additional emphasis. The proposed standard joined with the IS Auditing Guidelines G2 “Audit Evidence Requirement”, and G8 “Audit Documentation”, provide the level of

guidance necessary for the IS Auditor to achieve accurate and reliable audit results.

- c. The glossary on the first page states: “The words audit and review are used interchangeably.” These terms have very different meanings for CPAs in regard to levels of audit evidence and audit procedures used. We recommend that the meaning and use of the terms be more consistent with those used by other organizations, such as the AICPA.
- d. In addition, we feel that reference to the proposed standard, if issued, should be presented in S6 “Performance of Audit Work”, G2 “Audit Evidence Requirement” and G8 “Audit Documentation” (guide).

3. Please provide feedback on clause 03 and 04 (Standard).

In the standard, ISACA requires "03- The IS auditor should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results. "As indicated in question number 2, the terms "results" and "conclusions" are interchanged. An audit result is the opinion letter. An audit conclusion is what is in the opinion letter. In addition, the 'rebuttable presumption' that exists in GAAS asserting that audit evidence should also indicate that the work was done, etc., is absent from the ISACA standard.

4. Please provide feedback on clause 05 to 17 (Commentary).

- a. In the commentary on the proposed standard, ISACA states, "06- Audit evidence should be sufficient to enable an independent party to reperform the tests and obtain the same results. The level of documentation should be commensurate with the materiality of the item and the risks involved."

Comment: Levels of documentation should be completely divorced from the assessed level of risk or materiality. GAAS requires auditors to document all the auditor’s work regardless of the assessed level of risk or materiality associated with the assertion or statement the procedure examines. Accordingly, even low-risk assertions require audit evidence, but such evidence may be of a lower grade than high-risk assertions. To that end, audit evidence (e.g., analytical procedures) is still required.

- b. Relating reliability of evidence, ISACA states "09- Properties such as the source, nature (e.g., written, oral, visual, electronic) and authenticity (e.g., signatures, stamps, special media) of the audit

evidence should be considered when evaluating its reliability." [This goes on in more detail in section 10].

Comment: GAAS requires that external evidence, not the attributes of the evidence, (to) have the presumption of being more reliable. For example, according to the proposed standard a page with 3 signatures, which are internally generated, would be more reliable than an electronic acknowledgment from a bank on a bank statement. According to GAAS, evidence obtained independently from an external source is more reliable. In this case, the proposed standard is in direct contradiction to GAAS.

- c. Regarding cost/benefit, the ISACA proposed standards states "11- The IS auditor should consider the usefulness of the evidence and the cost required to obtain it. However, the difficulty and/or expense are not a valid basis for omitting a necessary process."

Comment: Paragraph 11 contains an internal contradiction. The proposed standard sets a test that can not be passed. If for example, an auditor decides that a procedure would be too expensive to perform, the auditor is allowed to omit that procedure. However, the second part of paragraph number 11 states that 'difficulty', presumably also costs or expense, are not a valid reason for omitting a procedure.

- d. ISACA's proposed standard: "16- Sufficiency is a measure of the quantity of audit evidence, while appropriateness is the measure of the quality of the audit evidence, and they are interrelated. In this context, when information obtained from the organisation is used by the IS auditor to perform audit procedures, the IS auditor should also place due emphasis on the accuracy and completeness of the information."

Comment: According to GAAS, materiality (which incorporates an assessed risk of misstatement) is the basis of selection of audit evidence and evaluation to deem (of) such evidence as sufficient. However, according to the proposed standard, (the) accuracy and completeness are the attributes that should receive due emphasis. The contradiction could lead to the following scenario: An auditor may reconcile or be satisfied with 99% of the material accounts that are contained in 2 lines but there are 1,000 immaterial lines that consist of the extra 1%. According to the proposed standard, the evidence would be insufficient because it would not be complete, if counting the total number of instances. The proposed standard then goes to discuss the accuracy without really resolving quantity vs. quality statement, which is contradictory to GAAS.

- e. Under section 05 Audit Evidence, 2<sup>nd</sup> bullet point, we recommend inserting “electronic and paper before source documents so that the statement would be changed to ‘includes electronic and paper source documents....’ This change highlights the point that the documents could be in a digital format.
  - f. Under Reliable Evidence, section 09, we recommend inserting “digital and manual” before signatures so that the statement would be changed to “e.g., digital and manual signatures....”.
  - g. Under Reliable Evidence, section 09, what is the meaning of the term “special media.” We recommend consideration of defining this term within the standard or at a minimum defining it in the ISACA glossary.
- 
-