ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008-3105, USA
Web Site: www.isaca.org

Telephone: +1.847.253.1545
Facsimile: +1.847.253.1443
E-mail: info@isaca.org

1 September 2011

Technical Director
International Auditing and Assurance Standards Board
545 Fifth Avenue, 14th Floor
New York, NY 10017

Via web site *www.iaasb.org*

Re: *Proposed International Standard on Assurance Engagements (ISAE)* ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information

Members of the International Auditing and Assurance Standards Board:

We very much appreciate the opportunity to provide comments and recommendations to the International Auditing and Assurance Standards Board *Proposed International Standard on Assurance Engagements (ISAE)* ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information. These comments and recommendations are offered on behalf of ISACA® and the IT Governance Institute® (ITGI®), international, independent thought leaders on information technology (IT) control, security and assurance, and governance of enterprise IT.

We are responding primarily from an IT perspective. We believe the *Proposed International Standard on Assurance Engagements (ISAE)* ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information will be useful to both member bodies and practicing external auditors and congratulate the IAASB on its accomplishment. Our general comments are provided in the following section of the letter and our responses to IAASB questions are included in Attachment A.

General Comments

We are very supportive of the IAASB *Proposed International Standard on Assurance Engagements (ISAE)* ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information. However, we offer the following suggestions.

The draft provides for two types of assurance engagements: reasonable assurance engagement and limited assurance engagement.

It appears that the definitions are designed for the assurance provider and not for the user of such assurance reports. Both of the definitions start with an indication that the practitioner reduces engagement risk to an acceptably low level, etc. What does that mean to the user of such reports and how does the practitioner clearly discuss the nature of the reports to the user (or the responsible party who is engaging the assurance provider)?

We suggest that it might be better if the definitions clearly describe the engagements and then describe what the provider of such reports needs to do to provide such levels of assurance. For example:

- 8.(a) (i) a. Reasonable assurance engagement—An assurance engagement in which the assurance provider (i.e., the practitioner) is able to provide a reasonable (high) level of assurance on the subject matter and the evidence examined to support the reasonable level of assurance. To provide this level of assurance, the practitioner performs sufficient procedures to reduce engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the practitioner's conclusion. The practitioner's conclusion...(continue with the wording in the existing paragraph).
- 8.(a) (i) b. Limited assurance engagement—An assurance engagement in which the assurance provider (i.e., the practitioner) does not provide a reasonable (high) level of assurance and provides only a limited level of assurance on the subject matter and the evidence examined to support the limited level of assurance. To provide this limited level of assurance, the practitioner performs a limited number of procedures to reduce engagement risk to a level that is acceptable in the circumstances of the engagement. The practitioner's conclusion is expressed in a form that conveys that, based on the procedures performed, nothing has come to...(continue with the wording in the existing paragraph).

  We also suggest that the Board consider expanding the limited assurance engagement to include those situations in which reasonable assurance cannot be provided because the nature of the subject matter, criteria or assurance procedures will not support reasonable assurance. This issue is discussed further in Attachment A, question 4.

* * * *

As the worldwide leading independent thought leaders on IT risk, governance and controls, we are eager to assist the IAASB in accomplishing its mission. We would be pleased to consider joint projects or other initiatives with the IAASB to help the IAASB achieve its strategies.

Please feel free to call on our organizations if we can be of assistance in any way on further deliberations, task forces or committees.

Again, we appreciate the opportunity to comment on the IAASB *Proposed International Standard on Assurance Engagements (ISAE)* ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information.

Respectfully submitted,

Michael P Bilger

Michael P. Bilger, CGEIT
Chair, Professional Influence/Advocacy Committee
ISACA (*www.isaca.org*)
IT Governance Institute (*www.itgi.org*)

About ISACA and ITGI

With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

The IT Governance Institute® (ITGI®) (*www.itgi.org*) is a nonprofit, independent research entity that provides guidance for the global business community on issues related to the governance of enterprise IT assets. ITGI was established by the nonprofit membership association ISACA in 1998.

Attachment A—Responses to IAASB Questions

ISACA/ITGI responses to the IAASB's questions are in *italics*.

The IAASB would welcome views on the following:

1. Do respondents believe that the nature and extent of requirements in proposed ISAE 3000 would enable consistent high quality assurance engagements while being sufficiently flexible given the broad range of engagements to which proposed ISAE 3000 will apply?

   Yes, we are supportive of the basic thrust of the proposed ISAE and believe that the requirements do provide appropriate flexibility. However, we believe that our recommendation in the following question 4. (b). would provide additional flexibility.

2. With respect to levels of assurance:

   (a) Does proposed ISAE 3000 properly define, and explain the difference between, reasonable assurance engagements and limited assurance engagements?

   See comments in the body of the letter regarding definitions.

   (b) Are the requirements and other material in proposed ISAE 3000 appropriate to both reasonable assurance engagements and limited assurance engagements?

   Consider different levels of assurance. With the types of engagements and the different levels of evidence available to support the assertions, it would seem that the IAASB should again be considering different levels of assurance on such assertions. Also, see the response underlined in question 4.

   (c) Should the proposed ISAE 3000 require, for limited assurance, the practitioner to obtain an understanding of internal control over the preparation of the subject matter information when relevant to the underlying subject matter and other engagement circumstances?

   We do not believe that obtaining an understanding of internal control as described in the question should be a requirement.

3. With respect to attestation and direct engagements:

   (a) Do respondents agree with the proposed changes in terminology from —assurance-based engagements‖ to —attestation engagements‖ as well as those from —direct-reporting engagements‖ to —direct engagements‖?

   Agree.

   (b) Does proposed ISAE 3000 properly define, and explain the difference between, direct engagements and attestation engagements?

   Yes. No further comments.

(c) Are the objectives, requirements and other material in the proposed ISAE 3000 appropriate to both direct engagements and attestation engagements? In particular:

(i) In a direct engagement when the practitioner's conclusion is the subject matter information, do respondents believe that the practitioner's objective in paragraph 6(a) (that is, to obtain either reasonable assurance or limited assurance about whether the subject matter information is free of material misstatement) is appropriate in light of the definition of a misstatement (see paragraph 8(n))?

Yes.

(ii) In some direct engagements the practitioner may select or develop the applicable criteria. Do respondents believe the requirements and guidance in proposed ISAE 3000 appropriately address such circumstances?

Yes.

4. With respect to describing the practitioner's procedures in the assurance report:

(a) Is the requirement to include a summary of the work performed as the basis for the practitioner's conclusion appropriate?

Yes.

(b) Is the requirement, in the case of limited assurance engagements, to state that the practitioner's procedures are more limited than for a reasonable assurance engagement and consequently they do not enable the practitioner to obtain the assurance necessary to become aware of all significant matters that might be identified in a reasonable assurance engagement, appropriate?

Consider whether there is a need for levels of assurance based not only on the amount of work performed, but also on the nature of the subject matter and the evidence to support such assertions.

For example, an assurance provider can provide assurance at a reasonable assurance level on commodities in a storage facility, where the practitioner can perform sufficient appropriate procedures to support such a level of assurance. However, an assurance provider may be able to provide only limited assurance on the recovery of a commodity in the ground, such as the amount of oil recoverable from tar sands (or a broad estimate of timber in a float based on aerial photos), regardless of the nature, number and timing of procedures performed. An IT example might be where the assurance provider is requested to provide a high level of assurance that hackers cannot penetrate the entity's human resource data stored in a cloud environment run by a start-up company. It would seem that there are many engagements in which the nature of the subject matter and criteria would or should lead to a limited assurance engagement. Perhaps this issue could be included as a subset of the limited assurance engagement, <u>particularly, as is stated in the draft, that the level of assurance conveyed by the practitioner can vary depending on the procedures performed</u>, etc. The limited assurance subset could also *include limited assurance engagements in which the assurance can vary depending on the nature of the subject matter, the criteria and the procedures that can be performed.*

In other words, the standard should limit the reasonable assurance to engagements that can be supported by objective evidence and adequate procedures performed by the practitioner, and provide for limited assurance where the practitioner:

1. *Is engaged to perform an engagement based on limited procedures*
2. *Cannot provide reasonable assurance because the nature of the subject matter, criteria or assurance procedures will not support reasonable assurance.*

(c) Should further requirements or guidance be included regarding the level of detail needed for the summary of the practitioner's procedures in a limited assurance engagement?

It may be appropriate, particularly if suggestion in response to question 4. (b). is followed.

5. Do respondents believe that the form of the practitioner's conclusion in a limited assurance engagement (that is,—based on the procedures performed, nothing has come to the practitioner's attention to cause the practitioner to believe the subject matter information is materially misstated‖) communicates adequately the assurance obtained by the practitioner?

A80. *Consider adding information on what, if anything, the practitioner would need to do to rely on the work of internal audit, or when relying on the work of internal audit is not appropriate.*

6. With respect to those applying the standard:

(a) Do respondents agree with the approach taken in proposed ISAE 3000 regarding application of the standard by competent practitioners other than professional accountants in public practice?

The approach is reasonable.

(b) Do respondents agree with proposed definition of —practitioner‖?

A96. and A168. *These paragraphs use the term auditor vs. practitioner.*

A109. *The last sentence of this paragraph is confusing in the context of the entire paragraph. Consider additional wording clarifying the three types of "experts."*

A practitioner's external expert is not a member of the engagement team and is not subject to quality control policies and procedures in accordance with ISQC 1.

A134. *The third bullet refers to being able to leverage experience gained during previous assurance engagements. Consider expanding this as a key point.*

Additional Comments

A 28. and A31. *These paragraphs (and others) address independence. There are subsequent references to this later. Consider adding a summary/table that indicates the type of engagements for which the practitioner would need to be independent.*

A35. *Consider stating whether the practitioner would ever include a written acknowledgment in the report.*

A50. *Consider defining "persuasive" and "conclusive."*

A57. *Consider adding a footnote indicating where the "IFAC's Member Body Compliance Program and Statements of Membership Obligations" can be obtained.*

A123. *Here the term "audit engagement" is used in the first and second bullet, yet it appears to refer to a direct engagement.*

A137. *The last sentence of this paragraph reads as if there is a word or two missing somewhere:* "If a further limitation is imposed the appropriate party(ies) after a limited assurance engagement has been accepted, it may be appropriate to withdraw from the engagement, where withdrawal is possible under applicable laws or regulations."

A140. *Consider stating whether a rep letter ever would be included in the report, in either a "short" form or a "long" form.*