17 May 2012

International Internal Audit Standards Board

Via e-mail: iia-exposure@theiia.org

Via web site: https://www.globaliia.org/standards-guidance/mandatory-guidance/Pages/2012-Standards-Exposure.aspx

Re: Standards Exposure

Members of the International Internal Audit Standards Board:

We very much appreciate the opportunity to provide comments and recommendations to the International Internal Audit Standards Board’s (IIASB’s) International Standards for the Professional Practice of Internal Auditing. 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, risk management, and governance of enterprise IT.

We believe the International Standards for the Professional Practice of Internal Auditing will be useful to practicing internal auditors and congratulate the IIASB on its accomplishment. Overall, the proposed revisions are relevant and timely. We have included our specific comments and our responses to IIASB’s questions in attachment A.

As the worldwide leading independent thought leaders on IT risk, governance and controls, we are eager to assist IIASB in accomplishing its mission. We would be pleased to consider joint projects or other initiatives with IIASB to help 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 IIASB’s International Standards for the Professional Practice of Internal Auditing.

Respectfully submitted,

John Ho Chi, CISA, CISM
Chair, Professional Standards 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—Considerations for IIASB Revisions

ISACA and ITGI fully support the IIASB revisions 1, 3, 9, 12, 13 and 17. ISACA/ITGI responses to the remaining IIASB revisions are highlighted below.

2. Change to Standard 1100
1100 - Organizational Independence
The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

Interpretation:
Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:

- Approving the internal audit charter;
- Approving the risk based internal audit plan;
- Approving the internal audit budget and resource plan;
- Receiving communications from the chief audit executive on the internal audit activity’s performance relative to its plan and other matters;
- Approving decisions regarding the appointment and removal of the chief audit executive;
- Approving the remuneration of the chief audit executive; and
- Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.

• Reviewing the performance of the audit function itself

Considerations:
- Remove the phrase “to the board” as illustrated above for simpler sentence structure without loss of content.
- Add the last bullet to emphasize the importance of board oversight of the audit function in maintaining organizational independence over time.

4. Change to Standard 1312
1312 - External Assessments
External assessments must be conducted at least once every five years by a qualified, independent reviewer assessor or review assessment team from outside the organization. The chief audit executive must discuss with the board:

- The need for more frequent form type of external assessments; and
- The qualifications and independence of the external reviewer assessor or review assessment team, including any potential conflict of interest; and
- The need for more frequent external assessments. Examples include changes to personnel, a significant business event or previous assessment results.

Considerations:
- Replace the term “form” in the first bullet with “type.” Given the global reach of the International Standards for the Professional Practice of Internal Auditing, the term “type” seems to be more easily translated than the term “form.”
• Add a final sentence as indicated to provide examples of factors that may trigger more frequent external assessments.

5. Change to Standard 1320

1320 - Reporting on the Quality Assurance and Improvement Program
The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.

Interpretation:
The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and the board and considers the responsibilities of the internal audit activity and chief audit executive as contained in the internal audit charter. To demonstrate conformance with the Definition of Internal Auditing, the Code of Ethics, and the Standards, the results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually. The results of the external assessment include the assessor’s or reviewer’s or review team’s assessment team’s evaluation with respect to the degree of conformance.

Consideration:
• Correct grammar in the first sentence of the interpretation.
• Revise the last sentence in the interpretation to shorten the sentence without affecting its meaning.

6. Change to Standard 2010

2010 – Planning
The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals.

Interpretation:
The chief audit executive is responsible for developing risk-based plans. The chief audit executive takes into account the organization’s risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization’s business, risks, governance, operations, personnel, programs, systems, and controls.

Considerations:
We agree that the change from “consultation” to “consideration” is a subtle, but very important revision. We further suggest to:
• Change “a risk-based audit plan” to “risk-based audit plans” to indicate the continuous quality of audit planning and the fact that audit plans do change over time.
• Remove the words “using” and “the” in the second sentence for clearer sentence structure without loss of content.
• Remove the word “senior” in the strike-out section.
• Add the terms “governance” and “personnel” as indicated.
• Organize the list of changes to clearly follow a structure, such as top-down, broader to more specific or risk-driven. Please also apply this consideration to 2120.a1 and 2130.a1 for consistency.
7. Change to Standard 2120.A1
2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems regarding the:
- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, standards, procedures, and contracts.

Consideration:
- Add “standards” to include this important corporate internal control component.

8. Change to Standard 2130.A1
2130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations, and information systems regarding the:
- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, standards, procedures, and contracts.

Consideration:
- Add “standards” to include this important corporate internal control component.

10. Change to Standard 2201
2201 – Planning Considerations
In planning the engagement, internal auditors must consider:
- The objectives of the activity being reviewed and the means by which the activity controls its performance;
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;
- The adequacy and effectiveness of the activity’s governance, risk management and control processes compared to a relevant control framework or model; and
- The opportunities for making significant improvements to the activity’s governance, risk management and control processes.

Consideration:
- Remove the word “processes” in the third and fourth bullets, since there may be controls that are not actually control processes.

11. Change to Standard 2210.A3
2210.A3 – Adequate criteria are needed to evaluate governance, risk management and controls. Internal auditors must ascertain the extent to which senior management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with senior management and/or the board to develop appropriate evaluation criteria.
Consideration:
• Add the word “senior” for consistency.

12. Change to Standard 2440
2440 – Disseminating Results
The chief audit executive must communicate results to the appropriate parties.

Interpretation:
The chief audit executive is accountable or designee reviews is responsible for reviewing and approves approving the final engagement communication before issuance and decides deciding to whom and how it will be disseminated.

Consideration:
• In the interpretation, replace “is responsible” with “is accountable.”

14. Change the definition of Board
The board is the highest level of governing body charged with responsibility to direct and oversee the activities and management of the organization. Typically, this includes an independent group of directors (e.g., a board of directors, a supervisory board, or a board of governors or trustees). If such a group does not exist, the “board” is the head of the company or agency. “Board” may refer to an audit committee to which the governing body has delegated its authority.

Consideration:
• In the definition, add the highlighted verbiage to create a complete sentence.

15. Change the definition of Controls Processes
Controls are the policies, standards, procedures, and activities that are part of a control framework, designed to ensure that risks are contained within the level of risk tolerances established by the risk management process, that an organization is willing to accept.

Considerations:
• In the heading, replace the term “Control Processes” with “Controls.”
• In the definition, add “Controls are the” to the definition to create a complete sentence.
• Add the term “standards” to the definition to capture this important corporate internal control component.

16. Add the new definition of Engagement Opinion Results
Engagement results consist of the ratings, conclusions, or other descriptions of results the outcome of an individual internal audit engagement based upon the procedures performed, relating only to those aspects within the objectives and scope of the engagement.

Considerations:
• In the heading, replace the term “Opinion” with “Results” to be consistent with other standards that were not part of the exposure draft summary.
• Add “Engagement results consist of” at the beginning of the definition to create a complete sentence.
• In the definition, replace the term “results” with “the outcome” to avoid a circular definition.

18. Delete the definition of Residual Risk
19. **Change the definition of Risk**

The possibility of an event occurring that will have an effect on the achievement of objectives, measured in terms of likelihood and impact. **The impact of the event may be positive or negative.**

Risk is the effect of uncertainty on organizational objectives. An effect is a deviation from the expected and may be positive or negative. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.

**Considerations:**
- Retain the original definition, since it seems more practical/pragmatic than the proposed change and enhance as follows:
  - Replace the first occurrence of “impact” with “effect.”
  - Restructure the sentence as indicated to focus on likelihood first, then on the impact, to better align with the risk assessment process.
  - Add the sentence “The impact of the event may be positive or negative.” to provide a balanced view of risk.
- Should you retain the new, proposed definition, edit as indicated to create a complete, first sentence.