

December 28, 2012

Information Systems Assurance and Control Association (ISACA)
ISACA Professional Standards Committee
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Response e-mailed to standards@isaca.org

RE: Response to the Information Systems Assurance and Control Association (ISACA) – Invitation to Comment (ITC) - “IT Audit and Assurance Standards”

Dear Sir/Madam:

The Institute of Internal Auditors (IIA) appreciates the opportunity to respond to ISACA’s ITC on “IT Audit and Assurance Standards.” We applaud the ISACA’s effort in soliciting feedback from diversified stakeholders. Our comments are based on a thorough analysis and discussion, utilizing a core team of IT audit experts who serve on The IIA’s Professional Issues Committee (PIC). These individuals consist of Certified Information Systems Auditors, Certified Internal Auditors, Certified Public Accountants, Chartered Accountants, audit executives and consultants who have worked in both public accounting and management positions in small, medium and large multinational organizations.

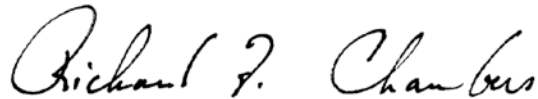
The following are our principal comments regarding the ITC. Our detailed comments are located in Appendix A and are broken down into two types: general and standard specific. General comments apply to all standards while standard specific comments apply to the standards noted in our commentary. In addition, our responses to the 20 survey questions are summarized in the Survey Questions Response section in the Appendix A.

1. The proposed change from “Information Technology (IT) audit/assurance professional” to “Information Systems (IS) audit/assurance professional” does not reflect the current state of the profession. The proposed change from IT to IS appears to be incongruent with ISACA’s Information Technology Assurance Framework (ITAF) since the framework itself uses Information Technology in the title as opposed to Information Systems. We believe the ITAF and the standards should be consistent.
2. The ISACA standards should contain a clear definition and consistent use of advisory services. While the proposed changes to the standards provide adequate coverage of audit or assurance services, they do not include advisory services provided by the IT audit professional. Advisory services are different from assurance services in various respects, but the primary difference is assurance or audit services are designed to determine the control adequacy and effectiveness of a given audit scope. Advisory services are consultative in nature where the client is provided guidance on an area or subject without the performance of audit procedures.

3. Consideration should be given to removing the terms “opinion”, “unqualified opinion”, “attest”, and “attestation” from the standards. These terms apply to audit engagements and audit professionals governed by the American Institute of Certified Public Accountants (AICPA) and non-US equivalents. If ISACA were to provide standards and guidance to its members on how and when an “opinion” could be expressed in written reports to management, these terms could be appropriate under these conditions.
4. There are a number of gaps in the proposed Standard 1008. We suggest ISACA consider adopting IIA Standard 1000 and the related 1000 series of Standards and PA 1000-1. The Standards collectively serve the profession of internal audit with respect to the required components of an Internal Audit Charter. Using the same language in ISACA and IIA Standards to present the required components of an Internal Audit Charter would help simplify the charter development process for internal auditing organizations.

The IIA would like to work with ISACA to help support those ISACA projects and standard setting activities related to the core competencies of internal auditing: governance, risk management and control. We value the opportunity to collaborate, share, contribute and learn. We welcome further discussion on any of these recommendations and offer our assistance in the continued development of these projects.

Best Regards,

A handwritten signature in cursive script that reads "Richard F. Chambers".

Richard F. Chambers, CIA, CGAP, CCSA, CRMA
President and Chief Executive Officer

About The Institute of Internal Auditors

The IIA is the global voice, acknowledged leader, principal educator, and recognized authority of the internal audit profession and maintains the International Standards for the Professional Practice of Internal Auditing (*Standards*). These principles-based Standards are recognized globally and are available in 29 languages. The IIA represents more than 180,000 members across the globe and has 107 affiliates in 190 countries that serve members at the local level.

Appendix A

General

1. All terms or definitions could be moved or consolidated into a glossary format. Having all “terms” in a glossary removes the redundant use in the proposed format which also removes the possibility of potential errors or inaccuracies of repeated terms between the standards.
2. The word “auditee” is outdated and contains a bit of a negative connotation. Consideration should be given to replacing “auditee” with “client” which is more positive and further advances the profession.
3. Reword the definition of the term “irregularity” to make it clearer that an irregularity could be intentional or unintentional.

Standard Specific

Standard 1001 – 2nd Commentary bullet: We recommend changing the wording to “be independent in fact and appearance.”

Standard 1003:

1. **Number 1 under Statement:** We recommend removing the term “opinion” as noted in the cover letter.
2. **Number 3 under Statement:** Reword to the following: “IT audit communicates management’s roles and responsibilities for each audit with respect to the provision of appropriate, relevant, and timely information required to perform the engagement.” It is not the role or the responsibility of IT audit to ensure management understands its obligations on each audit.
3. **6th Commentary bullet:** We recommend removing the phrase “unqualified opinion” as noted in the cover letter.
4. **6th Commentary bullet:** Remove the phrase “restrictive report.” The scope of an audit can be restricted and as a result, the report addresses the scope of the audit procedures performed, nothing more or nothing less. Therefore, enhance the wording around scope restrictions and not report restrictions.
5. **7th Commentary bullet:** Insert the word “a” before readiness assessment.
6. **7th Commentary bullet:** Insert the word “engagement” after advisory.

Standard 1004 – 4th Commentary Bullet: We recommend changing the wording to “all concerns related to application of standards should be appropriately addressed during the conduct of the IT audit engagement.”

Standard 1005:

1. The 4 bullets in the standard should be grouped together with the first sentence reading as follows: “The IT audit professional shall individually or collectively.”
2. **4th Bullet in the Standard section:** Anything can be audited but the question is the value of the audit and cost of the audit. We suggest rewording to make this clear.
3. **1st Bullet in the Commentary section:** Take out the phrase “are available” as resource availability is not a proficiency or skill set.
4. Strike the entire “Be prepared” section as it does not add value to the standard or the commentary.

Standard 1006: Add the word “management” to the assertion wording in the standard definition. This will make it clear the assertions are being made by management and not some other body.

Standard 1007:

1. **4th bullet in the Commentary section:** Change the word “they” to “it.”
2. **Publicly available section:** Add the Institute of Internal Auditors (IIA).

Standard 1008: Due to the number of gaps in this proposed audit standard, ISACA should consider adopting, whole or in large part, IIA *Standard* 1000 and the related 1000 series of *Standards* and PA 1000-1. The *Standards* collectively serve the profession of internal audit with respect to the required components of an Internal Audit Charter.

Standard 1201 – Commentary section: No need to differentiate internal versus external engagements as the planning and communication processes are the same.

Standard 1202:

1. Add residual risk definition to “terms.”
2. Consider adding verbiage that would address the fact that IT audit planning could be part of an integrated audit plan as opposed to a stand-alone plan.
3. Change opening sentence on the term “Audit Subject Matter Risk” to the “Risk relevant to the area under review, potentially including.”

Standard 1203 – 4th Commentary Bullet: We recommend removing the word “attestation” as noted in the cover letter.

Standard 1204:

1. **4th Commentary Bullet:** Change the wording to “...whether a control deficiency or combination of control deficiencies is a significant deficiency or a material weakness.”
2. **12th Commentary Bullet:** Change the wording to “...identify compensating controls and evaluate their design and operating effectiveness when determining whether ...”

Standard 1205: Remove the word “experts” from the standard and replace with “using the work of others.”

Standard 1206 – 6th Commentary Bullet: Reword to “...select the most appropriate procedure for the IT audit to achieve the engagement objective.”

Standard 1207:

1. **2nd and 10th Commentary Bullets:** Include significant weaknesses in conjunction with material misstatements.

Standard 1402:

1. **8th Commentary Bullet:** Reword to “...risk management framework and risk register are updated.”
2. Include a definition of risk register.

Survey Questions Response

Question 1: Agree.

Question 2: N/A.

Question 3: Uncertain.

Question 4: Please refer to our comments in the cover letter and General and Standard Specific sections in Appendix A.

Question 5: Uncertain.

Question 6: Please refer to our comments in the cover letter and General and Standard Specific sections in Appendix A.

Question 7: Agree.

Question 8: N/A.

Question 9: Agree.

Question 10: While we believe all of the proposed standards are relevant to the profession of IT audit, we also believe that virtually all of the proposed standards are applicable to the auditing profession in general.

Question 11: Agree.

Question 12: N/A.

Question 13: Agree.

Question 14: Please refer to our comments in the cover letter and General and Standard Specific sections in Appendix A.

Question 15: If ISACA believes the use of opinions should be included in the standards, consideration should be given to developing a standard and supporting guidance be created to instruct IT audit professionals on how, when and the conditions under which “opinions” could be provided.

Question 16: Yes.

Question 17: Please refer to our comments in the cover letter related to proposed ISACA standard 1008 and IIA *Standard* 1000, nature of the inconsistency and the suggested resolution.

Question 18: Strongly Disagree.

Question 19: Please refer to our comments in the cover letter and General and Standard Specific sections in Appendix A.

Question 20: N/A.