Richard F. Chambers
Certified Internal Auditor
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
President and Chief Executive Officer

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

April 12, 2013

Chartered Institute of Internal Auditors
Committee on Internal Audit Guidance for Financial Services
13 Abbeville Mews
88 Clapham Park Road
London SW4 7BX

Attn: Mr. Chris Spedding, Secretary to the Committee

Responded via email to chris.spedding@iia.org.uk

RE: Chartered Institute of Internal Auditors Consultation Document: Effective Internal Audit in the Financial Services Sector ("the Consultation Document")

Dear Mr. Spedding,

The Institute of Internal Auditors (IIA), the global standard-setting and certification body supporting its affiliates and members around the world, including the Chartered Institute of Internal Auditors (CIIA), appreciates the opportunity to respond to the committee established by the CIIA ("the Committee") to create new guidance for the UK financial services sector. We appreciate the significance of concern over failings in the financial system and applaud the Committee's effort to improve the performance and effectiveness of internal auditing in this sector, as evidenced by the Consultation Document.

Like the Committee, The IIA believes that a properly structured internal audit function, with robust *Standards* and guidance, can provide independent, objective assurance and advisory activities that add value and improve an organization's operations. To evaluate the Consultation Document, we formed a team of governance, compliance and internal audit practitioners, many of whom serve on The IIA's Standards Board and Professional Issues Committee, to analyze, discuss and respond within the exposure period. These individuals consist of Certified Internal Auditors, Certified Public Accountants, audit executives and consultants who have worked in both public accounting and internal audit leadership positions in small, medium, large and multinational organizations.

The IIA understands that the Committee's plan is to promulgate a "Code of Practice" ("Code") for financial services internal auditors, by outlining good practices and minimum requirements, consistent with The IIA *Standards*. And, we further understand that this Code may form the basis for future regulatory requirements in the UK. With this in mind, we offer our observations predominately in the context of where the Consultation Document appears to depart from IIA *Standards* and, therefore, may need to be revised. Our team of practitioners was also able to identify certain proposed recommendations that may pose significant, and perhaps unanticipated by the Committee, implementation challenges. We offer observations in this regard as well.

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org
www.globaliia.org

We commend the good recommendations made by the Committee to the CIIA for internal audit practitioners in the UK financial services sector. These recommendations cannot be mandated by the CIIA, as mandatory guidance or "standards" are outside the remit of any of the affiliates of The IIA, and would be a breach of the agreements affiliates of The IIA are bound to uphold. It is important that the guidance align as closely as possible with the International Professional Practices Framework (IPPF) in order to avoid confusion and ensure the guidance is widely adopted. To that end, we also have suggested a format in the Appendix for the Committee's consideration in communicating the final Code to clearly demonstrate its alignment with the *Standards*.

The following summarizes our principal comments.

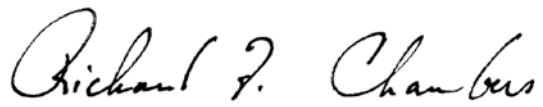
1. While the thirty-three recommendations are presented as guidance, they are written in the style of rules or requirements. As absolute rules, some of the recommendations impose hard line requirements that may not be possible for all organizations to implement, at least without significant cost. For example, Recommendation B3e directs internal auditors to "…evaluate whether the organisation is acting with integrity in dealings with **all** [emphasis added] customers and in its interactions with relevant markets." For most organizations, it is not possible to assess integrity in dealings with all customers. Although we believe principles-based standards are preferable, to the extent specific rules and guidance are desired, perhaps a "comply or explain" approach should be considered. Such an approach would allow practitioners to explain an exception, presuming they comply with the underlying principle, but have justification for diverging from the rule.
2. A number of recommendations appear to be inconsistent with the existing global IIA *Standards* and International Professional Practices Framework (IPPF), or introduce new requirements not present in the *Standards*. For example, Recommendation D9 states "Internal Audit should not be part of, nor responsible for, the Risk Management, Compliance or Finance function." We understand and appreciate the Committee's effort to enhance internal audit independence; however, the *Standards* do not proscribe a specific organizational alignment, because safeguards protecting internal audit independence can vary by organization, and conflicts can occur regardless of where the internal audit function resides. The IIA believes independence is best managed with a high integrity chief audit executive at a senior position in an organization, working for an active board audit committee. Rather than specifying or restricting organizational structures, perhaps the Committee could consider embracing the principles laid out in the "Three Lines of Defense" model - namely that internal audit must be an independent monitoring and oversight function, separate from operational and associated compliance functions.
3. The Consultation Document does not address potential implementation questions, such as the scope of application and expected timeframe. Examples include: Will the recommendations apply to all financial services entities, or just specific sectors, such as banking? Will they apply only to UK-based entities, or all entities operating in the UK including the subsidiaries of multinational entities, or to an entire entity with some operations in the UK, even if headquartered outside of the UK? Will they apply to all organizations, or organizations of a specified size or maturity?

The Appendix elaborates on these and other observations with more examples provided to underscore certain points. We have chosen to only highlight examples in the Appendix, rather than articulate a long list of points at this time. However, we welcome the opportunity to directly participate with the Committee, the Chartered Institute of Internal Auditors, the Financial Conduct Authority, the Financial Policy Committee, and any other applicable party, for further discussion on each of the thirty-three recommendations, mutually sharing observations, in a joint effort to enhance clarity and applicability of the entire Code.

Given the magnitude of the financial crisis, as well as the risk, governance and control failings in the UK financial services sector, we also offer our resources to assist in identifying not only point-in-time, rules-based recommendations, but to more importantly identify the root cause of the failings and suggest additional approaches beyond the Code that would enhance internal audit accountability and performance not only in the UK, but globally.

In closing, we appreciate the opportunity to provide these observations and suggestions to the Committee. As noted, we believe further discussion is warranted and would be productive to clarify, enhance, and streamline the proposed recommendations in advance of final publication. The IIA stands ready to assist the Committee in this regard.

Best regards,



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 109 affiliates in 190 countries that serve members at the local level.

Appendix

Observations from The Institute of Internal Auditors

Sections 1 though 3 below provide examples of Consultation Document recommendations that we believe, if issued as exposed, could lead to confusion about the authoritative nature of this new guidance or its alignment with the *Standards*. To that end, we suggest the Committee consider an alternative format in communicating the final Code. We suggest the final Code first note each related *Standard*, followed by the associated recommended practice(s). We believe such a format would more clearly demonstrate the Code's alignment with the *Standards*, differentiate the mandatory requirements from the recommended guidance, and reinforce the practitioner's responsibility to follow the underlying principle and not just the rule. The IIA stands ready to collaborate with the Committee in the development of such a format.

1. Recommendations versus Requirements

The discussion about the proposed recommendations states they are incremental guidance to the existing internal audit *Standards*. Specifically, the Covering Letter states, "These recommendations for the most part supplement, rather than replace, the existing *Standards*." However, the context of the recommendations, and some of the specific wording, indicates they are to be considered requirements. For example, recommendation G29 mandates that conformance with these recommendations be a part of the external assessment of an internal audit function.

Consistent with the UK's approach to Corporate Governance standards, The IIA has generally followed a philosophy of writing mandatory *Standards* as principles for the internal audit professional to apply. The internal audit professional considers the risk within their organization, the industry, the maturity, and multiple other factors when applying the *Standards*, exercising his/her judgment. However, the proposed recommendations generally specify rules, more explicit than the *Standards* or guidance included in the IPPF. Unfortunately, there are sometimes situations where organizations comply with a rule, but not with the principle the rule is trying to reinforce. Therefore, to the extent specific rules and guidance are desired, perhaps a "comply or explain" approach would allow practitioners to explain an exception, presuming they comply with the underlying principle, but have justification for diverging from the rule.

A few examples where the requirements are written as rules follow:

- Recommendation B3e: Directs internal auditors to "…evaluate whether the organisation is acting with integrity in dealings with all customers and in its interactions with relevant markets." It is not possible to assess integrity with all customers.
- Recommendation B5: Directs internal auditors to ensure its risk assessments "…take into account potential future or emerging risks on a continuous basis." Recognizing that the Committee emphasizes the expectation that internal audit take a risk-based approach, we observe that risk assessments can be performed routinely, systematically, periodically, but not truly continuously. This requires further clarification.
- Recommendation F25: States "The Board of Directors should confirm in the annual report that it is satisfied that Internal Audit has the appropriate resources." The IIA concurs that such a disclosure would be useful, but as a rule it is too narrow and may not capture the related principle. Disclosure would be strengthened with a broader confirmation of other relevant factors pertinent to Board oversight, such as if internal audit has the appropriate scope, charter, quality, etc.

2. Inconsistencies with the IPPF

Although the stated purpose is to provide incremental guidance to the *Standards*, there are a few examples where the proposed recommendations appear inconsistent with the *Standards* and the Definition of Internal Auditing included in the IPPF. Two examples are:

- Recommendation A1: Role and mandate of Internal Audit: The statement of the "primary role in internal audit" focuses solely on the assurance activities. However, the IPPF defines internal audit as an assurance and consulting activity, and recognizes that internal audit's role goes beyond protecting assets to also improving operations and adding value. The IIA believes that all internal audit functions, including those in financial services, have a broader mandate than suggested by this section. While we recognize that it was likely the Committee's intention to offer a view of the areas where internal audit can provide the greatest primary value, the recommendation, as worded, might appear to limit the scope of internal audit. We believe the mandate of internal audit is broader than helping protect assets, reputation, and sustainability, consistent with what is outlined in The IIA's Definition of Internal Auditing. Consequently, this may be an area where further clarification is warranted.
- Recommendation D9: "Internal Audit should be not part of, nor responsible for, the Risk Management, Compliance or Finance function." The *Standards* do not proscribe this organizational alignment for internal audit, as safeguards protecting internal audit's independence can vary by organization. The *Standards* provide the principles that independence must be maintained in appearance and substance, but purposely allow flexibility based on the nature and risk of different organizations. The implementation of such a rule could lead practitioners to be part of an organization other than Risk Management, Compliance, or Finance, but still independence impairing, such as operations. In addition, this recommendation is inconsistent with an IPPF Position Paper, "The Role of Internal Auditing in Enterprise-wide Risk Management."

  The IIA supports the principles laid out in the "Three Lines of Defense" governance model. Perhaps the Committee could consider embracing the principles laid out in that model, namely that internal audit must be an independent monitoring and oversight function, separate from operational and associated compliance functions, rather than specifying or restricting organizational structures.

3. Incremental Guidance

Although the recommendations are positioned to be incremental to the *Standards*, in many areas they seem to restate, albeit differently, the *Standards*. This creates an opportunity for confusion – should the proposed recommendation or the *Standard* be followed? Examples of recommendations that appear to be an attempt to restate a *Standard* are: 5, 6, 7, 14, 16, 22, 24, and 27.

4. Implementation of the Recommendations

As the final Code is prepared, we suggest the following implementation questions be addressed:

a. How "all significant risks," (as mentioned in Recommendation 1), is to be defined since the term "significant" is subject to interpretation. As well, the adjective "all" raises expectations that, even with best efforts, may not be achievable in practice.
b. Clarification of scope and applicability to all financial services entities, or just specific sectors, such as banking and insurance.
c. Applicability to all entities operating in the UK including the subsidiaries of multinational entities, or to an entire entity with some operations in the UK, even if headquartered outside of the UK.

d. Implication of the size or maturity of an organization in applying the guidance. The Covering Letter specifies the guidance may not be applicable to smaller institutions but 'smaller' is not yet defined.
e. Applicability to persons outside the internal audit profession when those persons are covered by a recommendation.
f. How to balance the cost and time required to comply with the recommendations when compared against the expected benefits.

As several of the proposed recommendations impact boards and/or audit committees, we also encourage the Committee to solicit and consider feedback from those groups, if not already solicited.