The Institute of Internal Auditors

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

March 28, 2014

Amy S. Friend
Senior Deputy Comptroller and Chief Counsel
Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street, SW, Suite 3E-218
Mail Stop 9W-11
Washington, DC 20219

Dear Ms. Friend,

RE: OCC Guidelines Establishing Heightened Expectations for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFR 30 and 170 – Docket ID OCC-2014-0001 (Guidelines)

On behalf of the over 180,000 global members of The Institute of Internal Auditors (The IIA), I am pleased to provide our observations and comments on the Office of the Comptroller of the Currency (OCC) proposed Guidelines Establishing Heightened Expectations for Large Banks. As the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, principal educator and, importantly, sole global standards setting body, it is with appreciation that we take this opportunity to provide comment on these proposed Guidelines. The IIA fully supports establishing standards for the design and implementation of an institution's risk governance framework, as well as providing standards for oversight of that framework by the board of directors.

In the United States, financial institution members make up the largest sector of our membership, and are supported by a specialty group overseen by The IIA's Financial Services Advisory Board (FSAB). Hence, our comments are based on input from leading financial institution internal audit practitioners and other noted thought leaders in the profession, combined with insights from our global purview.

Our primary comments related to the proposed Guidelines follow.

Overall we are supportive of the Guidelines, and find them consistent with practices many large banks follow today. They have been constructed in a way that offers a good balance of high level principles with sufficient detail in most circumstances to provide general direction. Among the many points where we could articulate our strong support, we specifically note the importance the OCC has placed on the key governance role internal audit plays, as well as signaling the importance of linking strategy and risk, by requiring that:

- "… the independent risk management and **internal audit** units must have unfettered access to the Board, or a committee thereof, with regard to their risk assessments, findings, and recommendations …" (page 16)
- "In carrying out their responsibilities within the Framework, front line units, independent risk management, and **internal audit** may engage the services of external experts to assist them. Such expertise can be useful in supplementing internal expertise and providing perspective on industry practices." (page 16)
- "The CEO should oversee the development of a written strategic plan with input from front line units, independent risk management, and internal audit." (page 25)
- "At a minimum, the strategic plan should cover a three-year period and should **contain a comprehensive assessment of risks**…" (page 25)

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

Additionally, we offer some points (below and in Attachment A) for your consideration. Principally,

1) **The Guidelines state, "Internal audit should also establish and adhere to processes for independently assessing the design and effectiveness of the Framework. The assessment should be done at least annually and may be conducted by internal audit, an external party, or a combination of both. The assessment should include a conclusion on the Bank's compliance with the Guidelines and the degree to which the Bank's Framework is consistent with leading industry practices."**

   We fully concur that internal audit should provide an independent assessment on the design and effectiveness of the Framework. However:

   - As the design of the Framework is not likely to change, or at least materially change, frequently, it may not be necessary to assess the design of the Framework annually. Internal audit should decide how to assess the design and effectiveness of the Framework based on its Board or Audit Committee endorsed risk-based internal audit methodology and attendant audit plan, and set the frequency of design and/or effectiveness assessment consistent with that risk-based view.
   - Whether the assessment is conducted by internal audit, an external party, or a combination of both, the assessment engagement should be overseen by internal audit, and the results reported by internal audit to those who are charged with governance. An external party leveraged to augment any competency gaps internal audit may possess in performing such an assessment is wholly consistent with IIA *Standards*.
   - As there is no authoritative source for leading industry practices, it may be difficult, if not impossible, for internal audit to conclude on the degree the Bank's Framework is consistent with leading industry practices. Rather, internal audit should conclude whether the design of the Framework is sound for the needs, challenges, risks and complexities of the Bank, as well as whether the Framework is operating effectively in light of that design.

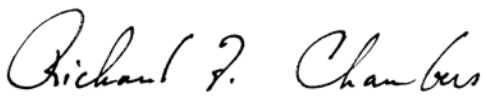
2) **In the section on "Risk appetite review, monitoring, and communicating processes" (page 28), the Guidelines require "independent risk management to monitor the Bank's risk profile in relation to its risk appetite and … report to the Board…" And, in the section on "Relationship of risk appetite statement, concentration risk limits, and front line unit risk limits to other processes" (page 31), it requires "…independent risk management to incorporate these elements into their strategic and annual operating plans…"**

   In both cases, we believe there is an opportunity for internal audit to play a key role in providing independent oversight on these important risk management activities. In monitoring risk management activities, internal audit can provide objective assurance to the Board, or appropriate Board committee, on the effectiveness of risk management. Leading internal audit functions do this today, consistent with the heightened expectations the OCC has of the largest banks under its jurisdiction.

Please do not hesitate to contact Glenn Darinzo, IIA's Director of Standards and Guidance, if you have any questions about this response and/or would like to schedule a time for us to either meet in person or via conference call. Mr. Darinzo can be reached by email: glenn.darinzo@theiia.org or phone 1-407-937-1164.

We fully support the efforts of the OCC to promulgate guidance for the promotion of standards for a risk governance framework within financial institutions. We have a shared interest and vested stake in enhancing good governance through effective risk management, as part of promoting stability with banks, other financial institutions, and all organizations. Consequently, we look forward to enhancing our relationship and future collaborations with the OCC.

Best Regards,



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

Attachment A
Specific Recommendations/Comments

	Recommendations/Comments
Responses to Questions #1 - #5	
1.	The OCC requests comment on the proposed conditions for determining whether a Bank's risk profile is substantially the same as its parent company's risk profile. • Banks with multiple bank subsidiaries would be penalized unless all bank subsidiaries could be combined to determine the 95%. We recommend that the guidelines be modified to include this combination. Also, we recommend that consideration be given to lowering the guideline to something less than 95% (e.g., 85% or 90%), which will be potentially more manageable and still remain at a suitably material threshold.
2.	The OCC requests comment on the advantages and disadvantages of having a single CRE, such as a Chief Risk Officer, provide oversight to all independent risk management units versus having multiple, risk-specific CREs providing oversight to one or more independent risk management units. • We believe that a single CRE or CRO would help to ensure a single cohesive and coordinated approach to risk management. Most banks already have a single CRE with deputies imbedded in the lines of business, which appears to be evolving as leading practice.
3.	Section II.C.3. (a) Provides that internal audit should maintain a complete and current inventory of all of the Bank's material businesses, product lines, services, and functions. The OCC requests comment on whether the Guidelines should provide that independent risk management also maintain such an inventory in order to ensure that internal audit has identified all material businesses, product lines, services, and functions. • We believe that this guideline may create some confusion as it implies that independent risk management should be reviewing, monitoring or inspecting the inventory maintained by internal audit. Conversely, this inventory should be maintained by independent risk management with internal audit auditing the inventory and providing assurance that the inventory is appropriately comprehensive. As the 3rd line of defense (LoD) in an organization, internal audit should be in the position of reviewing, evaluating and providing assurance on the work of 2nd LoD functions, such as risk management.
4.	The OCC requests comment on whether internal audit's assessment of the Bank's Framework should include a conclusion regarding whether the Framework is consistent with leading industry practices. Is such an assessment possible for internal audit given the wide range of practices in the industry and the challenges associated with determining what constitutes a leading industry practice? Are there any other concerns with such a requirement? • We believe that internal audit should provide an independent assessment on the design and effectiveness of the Framework. However, it should not be required that internal audit conclude as to the degree to which the bank's Framework is consistent with leading industry practices. Since there is no authoritative guidance, widely available source or body of knowledge to conclude on what is or is not leading practice, such an expectation should not be placed on internal audit in our view. • We recommend that the OOC provide more clarification on the requirement that internal audit assess the design and effectiveness of the Framework at least annually. It may not be necessary to assess the Framework if no changes have taken place and, therefore, we recommend that a risk-based approach be taken to determine the frequency of Framework review.
5.	The OCC requests comment on the composition of a Bank's Board. The proposed Guidelines establish a minimum number of independent directors that should be on the Bank's Board. Is this an appropriate number? Are there other standards the OCC should consider to ensure the Board composition is adequate to provide effective oversight of the Bank? Is there value in requiring the Bank to maintain its own risk committee and other committees, as opposed to permitting the Bank's Board to leverage the parent company's Board committees? • As each Bank will need to determine for itself what an appropriate Board size is in terms of numbers of directors, we believe a minimum ratio of independent directors to total directors is more appropriate.
Specific Comments	
1.	Page 5 - It states, "… including the development and maintenance of strong audit and risk management functions. This expectation involves institutions comparing the performance of their audit and risk management functions to the OCC's standards and leading industry practices and taking appropriate action to address material gaps." We recommend that guidance be developed on how an institution would obtain information on "leading industry practices" as it relates to audit and risk management functions so that this comparison could be performed. One way to enhance the confidence that a Bank's internal audit function is performing consistent with leading practices is to **require** conformance with a globally-recognized set of standards. The IIA promulgates the sole set of such standards, as the International Standards for

Recommendations/Comments	
	the Professional Practice of Internal Auditing (the *Standards*). Conformance with the *Standards* requires an external quality assessment be performed at least once every five years and also requires an ongoing quality assessment and improvement process.
2.	Page 14 - In the definitions section, a CAE is defined as "… an individual who leads internal audit and is one level below the Chief Executive Officer (CEO) …" This implies that the CAE reports, at least administratively, to the CEO. As there may be cases where, based on organizational structure or governance design, reporting to the CEO administratively is not practical or feasible, we recommend a "comply or explain" approach requiring the Board, or suitable committee of the Board, approve the explanation for the alternative administrative reporting relationship for the CAE if such a reporting relationship exists.
3.	Page 22 - It states, "If internal audit reports to the Board's audit committee, the audit committee or its chair would fill the aforementioned role of the CEO." Internal audit has historically been and, in our view, will continue to be most effective if it retains a dual reporting relationship. The functional relationship should be to the Board or Board's Audit Committee, with the administrative relationship to a suitable C-suite executive, preferable in most cases to the CEO. This dual reporting relationship maximizes CAE and internal audit effectiveness, while preserving the ability needed to operate independently.
4.	Page 22 - It states, "Internal audit should derive these ratings from its Bank-wide risk assessments, and should periodically adjust these ratings based on risk assessments conducted by front line units and changes in the Bank's strategy and the external environment." Internal audit should **consider** adjusting its ratings based on other risk assessments, hence we suggest revising this to read, "…and should periodically **consider adjusting** these ratings…" We also recommend that internal audit should also consider the independent risk management's risk assessment, as well as risk assessments conducted by other 2nd LoD functions.
5.	Page 23 - It refers to "objective measures that enable the identification, measurement and monitoring of risk and internal control issues" be in the report to the Board. We suggest that directional examples of such "objective measures" be provided to aid in clarity of what may be considered acceptable.
6.	Page 24 – It states, "Internal audit should also establish and adhere to processes for independently assessing the design and effectiveness of the Framework. The assessment should be done at least annually and may be conducted by internal audit, an external party, or a combination of both." While it may be implied, we would suggest clarifying to specifically state that the external party should report to internal audit, and any conclusions of the independent assessment on the design and effectiveness of the Framework be represented by internal audit.
7.	Page 24 – It states, "Internal audit should also establish a quality assurance department…" We believe that quality assurance is a function within the internal audit activity and may or may not need to be a separate department.
8.	Page 25 – It states, "The CEO and front line units demonstrate support by welcoming credible challenges from independent risk management and internal audit and including these units in policy development, new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes." We strongly support all of these areas of inclusion, and would further suggest, due to their overall importance to the risk profile of a Bank, that both "strategic planning" and "merger and acquisition activity" be explicitly added to the list.
9.	Page 26 – It states, "The qualitative components of the Statement should describe a safe and sound "risk culture"…" We recommend that there is a reference to the FSB's Guidance on Supervisory Interaction with Financial Institutions on Risk Culture, or some other authoritative guidance that describes "risk culture."
10.	Page 27 – It states, "…these indicators are generally not useful in proactively managing risk." While not as useful, arguably, as leading indicators, lagging indicators can still be instructive, therefore, we recommend stating that lagging indicators may be "less helpful" rather than "generally not useful."
11.	Page 32 – It states, "… a CAE that possess the skills and abilities to **effectively implement** the Framework." It should be noted that, while having these skills and abilities for the CAE are important and appropriate, the CAE does not **implement** the Framework. As a result, we would suggest this be reworded to clarify the role of a CAE to be to **effectively evaluate, assess and provide assurance on the overall effectiveness of the Framework**, or some such similar language.
12.	Page 32 – It states, "…internal audit implement and adhere to an effective Framework." It should be noted that internal audit does neither implement nor adhere to a RAF, but evaluates, assesses and provides assurances as to the effectiveness of the Framework, and would suggest the language be revised to reflect this clarification.
13.	Page 32 – It states, "The programs (meaning compensation and performance management programs) should also ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit." While the level and severity of issues are critically important, we believe it should be the speed and diligence with which any identified issues and concerns are addressed as being more suitable for consideration in compensation plans and potential negative effects on remuneration plans. Therefore, we recommend that the focus be on the timeliness of correction of issues, as well as than about the severity.
14.	Page 35 – It states, "The training program for independent directors should include training on:…(iii) other topics identified by the Board." We recommend additional wording, so that it reads, "…other topics identified by the Board or recommended by independent risk management and/or internal audit."
15.	Page 41 – In the section on Independent Risk Management, we recommend to include a statement that independent risk management should coordinate with other 2nd LoD functions and internal audit.