March 28, 2014

Submitted Via Email: regs.comments@occ.treas.gov

Office of the Comptroller of the Currency
Legislative and Regulatory Activities Division
400 7th Street, S.W. Suite 3E-218, Mail Stop 9W-11
Washington, D.C. 20219

Re: ***Docket ID OCC-20014-0001;*** *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, Integration of 12 CFR Parts 30 and 170*

Dear Ladies and Gentlemen:

The American Bankers Association, Financial Services Roundtable, Institute of International Bankers and Securities Industry and Financial Markets Association (together, the Associations)[1] are pleased to submit comments on the Notice of Proposed Rulemaking (Proposed Guidelines) published by the Office of the Comptroller of the Currency (OCC).[2] The purpose of the Proposed Guidelines is to establish minimum standards for the design and implementation of risk governance frameworks of insured national banks, Federal savings associations, and insured Federal branches of foreign banks,[3] with average total consolidated assets of $50 billion or more (together, Banks)[4] and minimum standards for directors overseeing framework designs and implementation.

The Associations support the OCC's efforts to enhance the governance and risk management practices of Banks, including requiring strong senior management and board oversight, and a "Lines of Defense" risk governance structure with effective independent risk management and

[1] Further information about the Associations is available in Appendix B.
[2] 79 Fed. Reg. 4282 (January 27, 2014).
[3] For a discussion on the unique impacts of the Proposed Guidelines on Federal branches, both insured and uninsured, please refer to the comment letter submitted separately by the Institute of International Bankers.
[4] The OCC has also reserved the right to apply the Proposed Guidelines on a discretionary basis to insured institutions with average total consolidated assets of less than $50 billion. In addition, the OCC is considering whether it would be appropriate to apply the Proposed Guidelines to uninsured entities regulated by the OCC including, national trust companies, and Federal branches and agencies of foreign banks.

internal audit functions. Since the OCC developed its set of principles, known as "heightened expectations," to enhance its supervision and strengthen governance and risk management practices of the largest national banks and Federal savings associations, those institutions have invested significant resources to strengthen further their risk management programs. The "heightened expectations" program has proven to be an effective means of improving risk governance and ensuring that the sanctity of the national bank and federal savings association charters are preserved. The effectiveness of this program has been enhanced by recognizing the diversity of the institutions subject to the program, and allowing those institutions and designated examining staff to tailor the program to be commensurate with the size, complexity and risk profile of each institution.

Unfortunately, in translating the "heightened expectations" program into the Proposed Guidelines, the OCC has proposed an unnecessarily rigid and prescriptive approach, which seems to be premised on compartmentalizing a Bank within its holding company, and then compartmentalizing the risk management functions within a Bank, rather than establishing risk management principles and goals for Banks to meet. The Proposed Guidelines also incorporate some features -- perhaps unintentionally -- that are unclear, and a likely source of unintended adverse consequences for the safe and sound management of Banks and the efficient provision of financial services to customers. The cumulative effect of the Proposed Guidelines, as drafted, could actually detract from, rather than enhance, the goals of sound risk management governance -- goals that we share. Accordingly, as described in our comments that follow, we strongly urge that the Proposed Guidelines be revised to be more principles-based, so they can be flexibly and more effectively applied to different types of Banks, and that important drafting clarifications be made to avoid unintended consequences.

Key Concerns

I. The Proposed Guidelines set out an overly rigid and prescriptive rules-based risk governance framework that could detract from sound risk management and is unclear in crucial respects.

Overall, the Proposed Guidelines establish a set of very inflexible "one size fits all" requirements that do not adequately take into account the unique and varied mix of products and services, strategic objectives, and organizational structures of the range of Banks subject to the Proposed Guidelines. These Banks vary widely in their business models and areas of focus, including: regional, mono-line, wealth management, investment and brokerage, global, and service to particular customer segments. The overly restrictive requirements of the Proposed Guidelines could reduce the ability of Banks to manage risk by requiring the creation of overlapping systems and frameworks, and changing otherwise effective reporting lines.

Most concerning is that, in multiple respects, the Proposed Guidelines appear to be premised more on a goal of compartmentalization -- of a Bank within its holding company, and of the activities of the Bank into three neat and completely separate "Lines of Defense" -- than on the principles and goals of sound risk management. The net result is to make it difficult, or at best unclear, how a Bank may use risk management resources of its parent company to support and enhance risk management at the Bank level. Similarly, compartmentalizing all of a Bank's

activities into one of three "Lines of Defense" draws artificially bright lines that ignore the mix of functions performed. This compartmentalization also fails to acknowledge the benefit, for risk management purposes, of recognizing functions, such as compliance and legal, that do and should have a role in more than one "Line of Defense."

To enhance the effectiveness of the Proposed Guidelines, the Associations recommend that they be recast around the risk management principles and goals the OCC expects Banks to meet. This approach would recognize the diversity of institutions subject to the proposal and enable risk management programs to be tailored most effectively and efficiently to meet those principles and goals based on each Bank's unique facts and circumstances.[5] Such an approach would allow Banks, in consultation with their designated examination and supervisory staffs, to employ strong governance following appropriately flexible and scalable techniques to tailor those standards most effectively to each Bank's unique business model and risk profile. As described more fully below, the Associations provide several recommendations on how the Proposed Guidelines could be revised to be more principles-based and goal-oriented, and thereby most effective.

A. The Proposed Guidelines' attempt to compartmentalize the Bank apart from its parent company's risk framework ignores the benefits and resources available to the Bank and potentially weakens its overall risk structure.

The Associations fully support the principle and goal that large banking organizations' risk frameworks include policies and processes that provide for the separate identification, measurement, and monitoring of risks and risk management activities at the Bank level. Such information allows Bank management and the board, as well as designated examiners, to identify the Bank's risk profile as a separate entity and distinguish the Bank from its parent company and nonbank affiliates. These tools also enable Bank board and management to assess readily the impact that decisions made by the parent company or another affiliate may have on the Bank.

Unfortunately, the Proposed Guidelines seem to be based on an assumption that in order to execute on these important elements, a Bank should be compartmentalized within its holding company, unless some exception to that premise can be justified. Unless a Bank can demonstrate that its risk profile is "substantially the same"[6] as its parent company -- a high bar to reach -- a Bank must establish a completely separate risk framework from its parent company which, read literally, includes separate personnel, technology, systems, and data architecture. What a Bank must do to avoid this result, either in whole or part, is unclear. Isolating the Bank from the risk management framework structure and support of the enterprise in which it resides will have unintended adverse consequences. Siloed risk management frameworks can result in inconsistent, and, potentially, conflicting standards over time. Failure to have a consistent framework throughout the organization can result in gaps that increase risk to the Bank and weaken the enterprise as a whole. Moreover, requiring a completely separate framework, as

[5] OCC's Deputy Comptroller for Operational Risk noted that institutions' "organizational structure and reporting lines, policies and procedures, and oversight accountability and reporting can vary greatly in design and complexity from organization to organization." Remarks by Carolyn G. DuChene, Deputy Comptroller for Operational Risk, before the American Bankers Association Risk Management Forum, Baltimore, Maryland (April 25, 2013).
[6] 79 Fed. Reg. at 4297.

presumptively required under the Proposed Guidelines, would result in a duplication of systems and resources that is less effective and efficient than allowing parent company resources to be available to support the Bank's risk management efforts. The use of parent company resources and risk frameworks would be entirely consistent, if not encouraged, by the statutory requirements that a holding company serve as a source of strength for its subsidiary depository institutions.[7]

Bank risk frameworks are strengthened when integrated with parent company frameworks. Integration allows Banks to leverage processes, personnel, resources, and technology developed throughout the enterprise in an effective and operationally efficient manner that can be tailored to the Bank's needs and risk profile. For example, bank holding companies have invested significantly in risk and control assessment technology, concentration and counterparty monitoring structures, and interest rate and credit measuring systems that Banks use to improve their ability to manage risk.

As long as the Bank can demonstrate that it meets the principle of separate identification, measurement, reporting and effective management of the Bank's risk, how and to what extent a particular Bank draws upon, or is a part of its parent company framework, should be determined by the Bank in consultation with its supervisors and examiners. For example, a Bank should be allowed to make use of the resources and risk management program of its parent company, including the parent company's risk management, control, and support functions, or appoint a Chief Risk Executive (CRE) or Chief Audit Executive (CAE), or other officers and personnel at the Bank level, who also may have a similar title and function at the parent company level (i.e., "dual-hatting"). Parent company audit functions should be able to be leveraged to meet the Proposed Guidelines, and Banks should be permitted to use the resources provided by parent company management and board committees.[8]

The Associations recommend that the OCC revise the Proposed Guidelines to focus on the principle that risk frameworks should provide for the separate identification, measurement, monitoring, and management of Bank level risks, as outlined above. The final guidelines should clearly allow each Bank, together with its designated examiner and supervisory personnel, the ability to determine how to draw upon enterprise resources and risk frameworks to provide the structure and support the Bank needs to identify, manage, and monitor its individual risk profile most effectively based on the Bank's unique facts and circumstances.

B. The Proposed Guidelines' definition of "Front Line Unit" is a departure from well-established principles of "Lines of Defense" that could unintentionally reduce the effectiveness of Bank risk programs.

"Lines of Defense" is a risk management approach that outlines roles and responsibilities in an effective risk management framework.[9] "Lines of Defense" form a system of checks and

[7] Section 616(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), Pub.L.No. 111-203 (2010).

[8] We note that 12 CFR 363.1(b)(2) permits insured depository institutions, with total assets of $5 billion or more and a composite CAMELS rating of 2 or better, to satisfy the section's audit committee requirements through the bank's holding company audit committee.

[9] *See e.g.*, Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk* (June 2011) at 4; Basel Committee on Banking Supervision, *The internal audit function in banks* (June 2012) at 12-13; COSO *Internal Control- Integrated Framework* (May 2013).

balances whereby the first line is responsible for managing the risks it creates. The second line challenges the first line's "inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems."[10] Internal audit, the third line, is responsible for independently verifying that the Bank's risk framework is operating as intended. The Associations fully support the principles underlying the "Lines of Defense" concept, which is a tried and proven approach.

The Associations also strongly support the OCC's goal in ensuring that the stature and authority of the Independent Risk Management (IRM) function is sufficiently elevated within an organization to carry out its responsibilities effectively and to serve as a "check" on the actions taken by business lines. However, the Proposed Guidelines take a compartmentalized approach to applying the concept of "Lines of Defense," which may unintentionally limit the ability of a Bank's second line to meet that goal. As drafted, a Bank department or type of activity is either in the first, second, or third line, and any department or type of activity that is not considered a second or third line activity is lumped into the first line. This compartmentalization is novel, elevates the label or title of an activity or department over the actual functions involved, and ignores the value of having certain types of functions (e.g., compliance or legal) performed in more than one "Line of Defense."

Under the Proposed Guidelines, "Front Line Unit," which equates to the first line, is defined very broadly to include not only Bank business lines that engage in revenue generating and client facing activities, but also support and control departments and activities, including finance, treasury, legal, human resources, operations, information technology, and processing.[11] This new and novel definition represents a significant broadening and departure from well accepted forms of the "Lines of Defense" approach. The Basel Committee on Banking Supervision, for instance, recognizes the first line to comprise "business line management,"[12] and the second line may include control and "support functions, such as risk management, compliance, legal, human resources, finance operations and technology."[13] Distinguishing business lines in this manner is important, because the revenue generating focus of business units typically introduces the most significant risks to an institution. Thus, business line activities require the Bank's most robust set of checks and balances. Understanding the distinction allows institutions to deploy resources and focus in a risk-based and flexible manner on the areas of the Bank that pose the greatest risk.

Depending upon the Bank's business model and complexity, the second line can be comprised of certain functions in addition to IRM. Independent Bank-wide control and support groups, such as compliance, legal, information security, finance, treasury, and human resources, also may form a part of the Bank's second line because of the expertise and skills these functions bring to bear. As the Financial Stability Board recognized, "[c]onsidering the broad scope of operational risk and the three lines of defence, many financial institutions are moving toward a model whereby second line of defence responsibilities are formally assigned to other independent

[10] Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk* at 4.
[11] 79 Fed Reg. at 4297.
[12] Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk* at 4. We also appreciate Comptroller Curry's recognition of this concept by referring to "front line *business* units" as the first line of defense, in testimony before the Senate Committee on Banking, Housing, and Urban Affairs on February 6, 2014.
[13] Basel Committee on Banking Supervision, *The internal audit function in banks* at 12-13.

groups with sufficient expertise in these areas, such as Information Security, Privacy, Technology Risk Management, Corporate Security, Business Continuity, Compliance etc."[14] Given the complexity and technical nature of operational risk, Banks need to rely on internal experts to perform roles to oversee these risks effectively and efficiently. This is particularly true of a Bank's compliance function, which is virtually absent from mention in the Proposed Guidelines. Characterizing any of the above-listed groups as "Front Line Units" is counterproductive to sound risk management. In addition, requiring IRM to duplicate and replicate these functions is sub-optimal and detracts from IRM's responsibilities for overseeing the Bank's risk management program.

Defining Front Line Unit to include the Bank's legal department and activities further exacerbates the practical challenges underlying the Proposed Guidelines and will have significant impact on the authority and proper functioning of in-house legal departments. Like other support and control functions, legal provides a particular skill set and expertise that is vitally important to the proper functioning of both the first and second line.[15] Compartmentalizing Bank legal departments into the first line also raises unique issues as to whether IRM and Internal Audit (IA) are required to assess independently the risks posed by litigation involving the Bank or review the legal advice provided.[16]

The Associations recognize that the "Lines of Defense" framework is an effective means of checks and balances on the risk taking functions of a Bank. However, the goal of sound risk management will be better served through an approach premised on the principles and goals of what each of the "Lines of Defense" is supposed to do, and a recognition that the described support and control activities may support the goals of more than one "line" based on the structure, design, and complexity of the individual Bank's framework. Different aspects of these control and support activities can -- and should -- occur in more than one "line," based on the function performed, not merely the label. For example, overall compliance is strengthened if front line business units take responsibility for conducting business in a compliant fashion, a robust compliance function is part of IRM, and IA has compliance expertise to assess whether the foregoing compliance risk management functions are operating effectively. This is not to say that control and support functions do not require oversight and review, but what is appropriate needs to be calibrated to the function that the support area is performing. For example, a Bank could establish a program of oversight by IRM for a control unit's critical policies and high risk first line activities (e.g., a risk review of compensation plans and programs established by Human Resources). It is not necessary to focus on the titles of Bank departments and rigidly characterize these functions as Front Line Units, or change well established and effective reporting lines in order to ensure that appropriate oversight occurs.

---

[14] Financial Stability Board, *Increasing the Intensity and Effectiveness of SIFI Supervision: Progress Report to the G20 Ministers and Governors*" (November 1, 2012) at.14.

[15] Bank legal functions also assist the third line, for example, providing legal advice to audit regarding internal investigations, or advice on the Bank's compliance with laws and regulations. Bank legal functions also have broader corporate advisory responsibilities.

[16] Such a construct could also raise concerns about the protection of attorney client privilege, which we do not believe was intended under the Proposed Guidelines.

For these reasons we strongly recommend that sections I.C.3 (ii) and (iii) of the Proposed Guidelines be deleted and that the Guidelines incorporate a statement that the placement and treatment of the enumerated control and support activities in the risk governance framework will be based on the functions they actually perform relative to the role and goals of each of the "Lines of Defense."

C. The reporting line requirements of the Chief Audit Executive are too narrow and should permit alternative senior management reporting, when proper controls exist to protect Internal Audit independence and unfettered access to the Bank board.

The Associations are concerned that the Proposed Guidelines -- perhaps unintentionally -- depart materially from the Comptroller's Handbook: Internal and External Audits (the OCC Audit Handbook),[17] and the standards established by the Institute of Internal Auditors (IIA) with regard to the CAE's reporting line. Specifically, although the Proposed Guidelines provide for the Chief Executive Officer (CEO) or Audit Committee to oversee the CAE, the Proposed Guidelines do not provide for reporting flexibility to another senior executive, such as the General Counsel, on day-to-day administrative issues.

The OCC's Audit Handbook explicitly allows for a CAE to report to another senior executive on day-to-day administrative issues so long as the board "take[s] extra measures to ensure that the relationship does not impair the auditor's independence or unduly influences the auditor's work."[18] In addition, the OCC's Audit Handbook references the IIA, a well-established internal audit professional association, with regard to oversight and structure of the internal audit function.[19] The IIA standards recognize a flexible reporting structure by allowing that where a CAE does not report to the CEO, the CAE "must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities."[20]

The Associations recommend that the Proposed Guidelines be revised to provide formally for flexibility in the CAE reporting structure when the appropriate controls exist, such as those identified previously and formally by the OCC and IIA. Further, the Associations believe reporting line flexibility fully supports the goals of strong IA independence and unfettered access to the Bank's board.

D. Any required comparison of a Bank's risk management framework to "leading industry practices" would be unverifiable and subjective and may not be in the best interest of the Bank.

The preamble to the Proposed Guidelines specifically requests comment on whether IA should be required to conduct an assessment that includes a conclusion on the "the degree to which the Bank's Framework is consistent with *leading industry practices.*"[21] Strong IA programs that

[17] OCC Audit Handbook (April 2003).
[18] *Id.* at 23.
[19] *Id.* at 10.
[20] IIA *International Standards for the Professional Practice of Internal Auditing,* Standard 1110 - Organizational Independence.
[21] 79 Fed. Reg. at 4288 (emphasis added).

independently evaluate a Bank's compliance with regulatory requirements are vitally important to any effective risk management program. However, "leading industry practices" is a subjective requirement that IA and examiners would be unable to verify. IA would face significant challenges in trying to meet such a requirement, including the lack of any authoritative body responsible for determining leading risk management practices, and the difficulty in finding financial institutions willing to share their practices for comparative purposes. In addition, such a requirement could result in IA determining what risk management practices a Bank should institute, resulting, perhaps, in IA designing portions of the Bank's risk framework, thereby potentially impacting its ability to review the framework independently. Further, the most effective risk management programs are those that are tailored to the business model and complexity of the Bank and "leading" or "best" practices for some Banks may not necessarily be suitable for a particular Bank.

For the reasons stated above, we believe that any benefits that would be derived from trying to determine leading industry practices would not merit the cost of conducting such a review, which would undoubtedly require the hiring of consultants to conduct a cross industry comparison of risk management practices. The Associations strongly urge the OCC to remove the requirement that IA evaluate whether a Bank's risk framework is consistent with "leading industry practices" from the Proposed Guidelines and to clarify that the Proposed Guidelines are not intended to impose any obligation on a Bank that is different or in addition to the requirements contained in the existing OCC Audit Handbook.

E. Failure to coordinate with other agencies, particularly the Federal Reserve, on risk management frameworks for large institutions creates confusion and could weaken enterprise risk management.

Banks are subject not only to the risk management expectations and requirements of the OCC, but also, through their parent company, the risk management expectations and requirements of the Board of Governors of the Federal Reserve (Federal Reserve).[22] Differing terminology and expectations between the two agencies regarding risk management governance and framework requirements can create confusion for Banks as they try to reconcile the requirements of both regulators. To illustrate the point, the Federal Reserve expects institutions to have a consistent risk framework that flows from the top of the organization through the entire enterprise.[23] As a result, risk officers at the Bank level are expected to report into the parent company risk management function to ensure consistent risk culture and process throughout the enterprise. The Proposed Guidelines, however, require the CRE of the Bank to report to the Bank's CEO, potentially creating confusion about how the two requirements are to be reconciled.

[22] *See, e.g.*, Federal Reserve, *Enhanced Prudential Standards for Banking Holding Companies and Foreign Banking Organizations, Final Rule* 79 Fed. Reg. 17240 (March 27, 2014) (Final 165 Rule); Federal Reserve, Supervision and Regulatory Letter 12-17, *Consolidated Supervision Framework for Large Financial Institutions* (December 17, 2012) (SR Letter 12-17).

[23] The Federal Reserve expects each firm it regulates "to ensure that the consolidated organization (or the combined U.S. operations in the case of foreign banking organizations) and its core business lines" are financially resilient by maintaining, among other things, effective corporate governance and risk management programs. SR Letter 12-17.

Additionally, unlike the Proposed Guidelines, the Federal Reserve permits internal audit at the holding company level to report administratively to someone other than the CEO.[24]

The OCC has recognized in many contexts the importance of interagency collaboration on examination, supervision, and regulatory matters.[25] The Associations strongly urge the OCC also to recognize the importance of collaboration with respect to risk management frameworks and governance expectations, and to coordinate with the Federal Reserve on the requirements and expectations for large banking organizations, including the interplay between the Proposed Guidelines and the Final 165 Rule, as well as the implementation of such requirements.[26]

II. The description of the roles and responsibilities of the board of directors under the Proposed Guidelines represents a profound change in the duties of Bank directors and, as a presumably unintended consequence, in their exposure to personal liability, which will undermine the ability of Banks to attract the directors needed to carry out the risk governance role of the board most effectively.

A. The Proposed Guideline's expansive use of the word "ensure" seemingly requires Bank directors to "guarantee" outcomes -- an impossible task -- that will impact the ability of Banks to attract qualified board candidates.

The Associations fully support strong board oversight of Bank risk management frameworks. The board's oversight role includes: critical evaluation, review and approval of the Bank's material risk management policies; oversight of the Bank's risk framework; holding management accountable; and challenging management when necessary. However, the Proposed Guidelines appear to go beyond these baseline principles to require that each member of the Bank's board "*ensure* that the Bank establishes and implements an *effective* framework that complies with the Proposed Guidelines."[27] Such a requirement suggests that the board must in effect guarantee the outcomes under the Bank's framework, which is unrealistic and impractical. The Group of Thirty recently stated that supervisory guidance regarding board oversight:

> "…needs to respect the role of the board as separate from management. For example, it should avoid the use of the words '*the board ensure*,' in recognition of the role of the board, which is overseeing and satisfying itself through reasonable procedures that management is implementing board direction. '*Ensure*' is too high a bar to judge effectiveness…"[28]

---

[24] Federal Reserve, Supervision and Regulatory Letter 13-01, *Supplemental Policy Statement on the Internal Audit Function and its Outsourcing* (January 23, 2013).

[25] Comptroller Curry has stated that the OCC is "stepping up" coordination with other agencies, including the Federal Reserve and is making interagency collaboration one of his top priorities. Comptroller Thomas J. Curry, Remarks before the 49th Annual Conference on Bank Structure and Competition (May 9, 2013).

[26] For example, the OCC could permit dual reporting of the CRE to the Bank CEO and the Chief Risk Officer of the holding company.

[27] 79 Fed Reg. at 4291 (emphasis added).

[28] The Group of 30 *A New Paradigm: Financial Institution Boards and Supervisors* (October 2013) at *28* (emphasis added).

Holding directors to an unobtainable high bar will significantly impact the ability of Banks to attract qualified directors.

The Associations do not believe that the OCC's intent was to require directors to guarantee outcomes. To clarify its intent, the Associations recommend that the OCC modify the Proposed Guidelines to focus on the board's responsibility for oversight of management and the Bank's risk program, rather than on ensuring outcomes. We would suggest that the OCC more precisely describe the action the OCC expects Bank directors to take (e.g., the board must "require" management to implement a risk framework that meets the Proposed Guidelines that is commensurate with the Bank's business model, complexity and risk profile, must "oversee" management's implementation thereof, and hold management accountable for meeting the requirements of the established framework). Such an approach would also more closely align with the Final 165 Rule board risk committee requirements.[29]

B. The Proposed Guidelines go beyond well-established laws regarding corporate governance seeming, perhaps unintentionally, to create a new and untested fiduciary duty.

In discussing the sanctity of the charter and the OCC's prior guidance on "heightened expectations," the preamble to the Proposed Guidelines states that "one of the primary *fiduciary* duties of an institution's board of directors is to *ensure* that the institution operates in a safe and sound manner."[30] Although the Proposed Guidelines do not refer to "fiduciary duty," the Proposed Guidelines do state that the board "has a *duty* to oversee the Bank's compliance with safe and sound banking practices" and "should *ensure* that the Bank establishes and implements an effective risk governance framework that meets the minimum standards described in these Proposed Guidelines."[31]

Fiduciary duties long recognized in corporate and state law include the duties of care and loyalty. The duty of care requires "that directors act in good faith, with the level of care that an ordinarily prudent person would exercise in similar circumstances, and in a manner that they reasonably believe is in the best interest of the organization."[32] The duty of care requires directors to acquire sufficient knowledge of material facts, critically evaluate information available to them, and actively participate in the decision making process. The duty of loyalty "requires that directors exercise their powers in the interests of the organization" rather than the director's own interest.[33] The Associations agree that a Bank director's fiduciary duty of care and loyalty is to the Bank. However, the Proposed Guidelines mix the concepts of fiduciary duty and regulatory expectations in a way that creates significant concern and potentially increased liability for directors.

---

[29] Twelve C.F.R. Section 252.33(a) of the Final 165 Rule states that the holding company's risk committee is responsible for approving and periodically reviewing the holding company's risk management policies and overseeing the operation of the holding company's risk management framework. Fed. Reg. at 17318.
[30] 79 Fed. Reg. at 4283 (emphasis added).
[31] *Id*. at 4300 (emphasis added).
[32] OCC, The Director's Book (October 2010) at 78.
[33] *Id*.

Undoubtedly, Bank directors are subject to the expectations and requirements of regulators, but this is different from a fiduciary duty. To conflate the two is confusing and could be viewed as creating a new and untested "fiduciary" duty upon which claims of third parties could be based. This result would be an added detriment to the already challenging task of finding qualified individuals to serve as directors and, contrary to the goal of the Proposed Guidelines, to have informed, expert and active directors contributing to strong risk governance. Creating a new and untested duty, through Part 30, could also impact class action and shareholder derivative litigation and affect the cost, terms or availability of Bank director liability insurance.

C. Certain provisions of the Proposed Guidelines blur the distinction between Board oversight and management of day-to-day operational responsibilities, distracting the Bank board from its critical strategic and oversight responsibilities and overreaching into management personnel tasks.

One of the fundamental features of corporate governance is the distinction between the role of the company's board of directors and the company's management. The distinction permits a board to stand above and apart from the day-to-day operations of the company and thereby bring broader strategic and policy perspective, as well as independent judgment, to the company.

As recognized in the Proposed Guidelines themselves and the OCC's Directors Handbook, the director's responsibility is to "oversee" the Bank's operations including its compliance with safe and sound banking practices. The Federal Reserve too, in the preamble to its Final 165 Rule, recently addressed the oversight role of holding company board risk committees, stating that board risk committees must act in an oversight role, meaning that they must "fully understand the company's enterprise-wide risk management policies and framework and have a *general* understanding of the risk management practices of the company."[34]

The specific requirements placed on Bank directors under the Proposed Guidelines for talent management blur the lines between board oversight and Bank day-to-day management. The requirements for the Bank board to oversee the talent development, recruitment, and succession planning processes for the entire IRM and IA functions, appears to cross the line into management activities of departments with potentially hundreds of employees. Similarly, depending on the organizational structure of the Bank, requiring the board to oversee the talent development, recruitment, and succession planning processes for individuals two levels down from the CEO could include numerous Bank officers. The Proposed Guidelines requirement that the board establish reliable succession plans for the CRE and CAO also appears to be a management function. In addition, the term "processes" could be interpreted to include individual hiring and firing decisions, and personnel performance and development plans. The Associations agree that Bank boards should oversee the talent management, recruitment, and succession planning of key officers of the Bank, including the CEO, CRE and CAE, and that the board should have a general understanding of the Bank's talent management, recruitment, and succession planning processes for IRM, IA, and senior officers. However, requiring Bank boards to oversee talent development, recruitment, and succession planning processes of potentially hundreds of individual employees is clearly a management activity that goes well beyond the oversight function of the board. Accordingly, we recommend that the Proposed

[34] 79 Fed. Reg. at 17248 (emphasis added).

Guidelines (sections II.L.1 (iii) and I.L.2 (iii)) be revised to remove the talent management obligations of the board related to the talent development, recruitment, and succession planning processes of IRM, IA, and individuals two levels down from the CEO.

D. The Proposed Guidelines' inappropriate emphasis on documentation, opposition, and the negative aspects of "credible challenge" will detrimentally impact the relationships between boards and management, and reduce, rather than increase, effective interaction.

The Proposed Guidelines require that a Bank's board should provide active oversight of management.[35] In providing active oversight, according to the Proposed Guidelines, the board should "question, challenge, and when necessary, oppose recommendations and decisions made by management…."[36] Effective boards articulate to management their expectations regarding strategies, frameworks, and risk appetite in many formal and informal ways. Boards may ask for additional information or options, chairs of key committees meet with management periodically, and directors frequently have informal meetings with management seeking clarification or a better understanding of a particular proposal or plan. In most cases, management proposals that are outside of the board's expectations are not brought to the board for approval, and/or are not implemented because management already understands that they would conflict with board views.

The Associations are concerned, given the potential liability under the Proposed Guidelines, that "credible challenge" at Banks will become just a documentation exercise for examination purposes that will deter open and candid dialogue between the board and management. The Associations strongly urge the OCC to be clear in the Proposed Guidelines that verification of the expectations surrounding credible challenge should not hinge on documentation, but rather on all dimensions of interaction between the board and management, which can be – and are – evident from robust conversations between Bank board members, including independent directors, and examiners. Rather than a focus on documentation, examiners should look to board members, particularly the independent directors, to be able to articulate the risks facing the Bank, and confirm that board members have taken opportunities to raise any independent concerns they may have about the Bank's risk management.

The Associations are also concerned with the proposed requirement that the board "oppose" recommendations of management when necessary. We are concerned that placing an emphasis on board opposition in the Proposed Guidelines will take away from the intent of the Proposed Guidelines to evaluate how effectively the board probes management and how active the board is in overseeing management actions. Therefore, we recommend that the Proposed Guidelines be clarified to place less emphasis on opposition to management and documentation, and provide more clarity that the OCC will look to how credible challenge by the board is exercised in practice. Local bank examination teams, through ongoing assessments, engagement with board members, and review of minutes are best able to determine if credible challenge exists from the board.

[35] 79 Fed. Reg. at 4300.
[36] *Id.*

III. The OCC should not apply the Proposed Guidelines or similar requirements to OCC regulated insured institutions with assets less than $50 billion, at its option, but rather only through appropriate public rulemaking.

Under the Proposed Guidelines, the OCC "reserves authority" to apply the proposal to insured national banks, Federal savings associations, and Federal branches with total assets of less than $50 billion. The OCC states that it will apply the Proposed Guidelines, and Part 30, to these entities when it determines that an entity's operations are highly complex or "*otherwise present a heightened risk*."[37] Although the OCC does provide very broad factors, such as complexity of products and services, risk profile, and scope of operations that it will use in determining applicability of the Proposed Guidelines, the proposal provides little clarity at all to such an institution as to when it will apply. While we appreciate that in this one limited context the OCC recognizes that "one size fits all" is not an appropriate way to regulate institutions under the Proposed Guidelines, significantly greater clarity needs to be provided to institutions, and their directors and officers, who could be potentially subject, with little or no warning, to enforcement action for failure to comply. We strongly urge the OCC not to apply the Proposed Guidelines on a case-by-case basis and at its discretion to OCC regulated insured institutions with assets less than $50 billion. If and when the OCC determines it is necessary to apply the Proposed Guidelines to any additional OCC regulated insured institution, it should amend the guidelines through the notice and comment process, and establish clear criteria that could be used to determine when an institution is required to comply. We also strongly encourage the OCC to provide a separate notice and comment period if the OCC determines to formalize its "heightened expectations" for uninsured trust companies and Federal branches. Such guidance should be specifically tailored to the unique characteristics of these institutions.

In addition, as OCC regulated institutions become subject to the Proposed Guidelines in the future, the OCC should establish a reasonable time frame for institutions to become fully compliant. We recommend that when an institution becomes newly subject to the Proposed Guidelines that it be permitted a minimum of two years to achieve full compliance.

IV. The Proposed Guidelines, as drafted, will require significant and, in some cases, radical changes to reporting lines and functions, and a substantial increase in resources, requiring an extended implementation period.

Although the OCC has stated that the Proposed Guidelines are simply the formalization of the OCC's "heightened expectations" examination program, as we highlight above, there are new or more detailed requirements in the Proposed Guidelines. Banks will need time to review their existing frameworks to identify gaps and any changes that will be needed to be in full compliance with the Proposed Guidelines. Changes are likely to be required to systems, documentation, personnel, and reporting lines, which will take time to implement. As a result, the OCC should allow Banks subject to the Proposed Guidelines a minimum of one year from the date of the final rule to comply fully.

[37] *Id.* at 4297 (emphasis added).

In addition, there are some Banks that have not been subject previously to the "heightened expectations" examination program at all or only to certain aspects. The OCC acknowledges that the Proposed Guidelines "would be applicable to a broader group of institutions than those currently subject to the heightened expectations program."[38] These institutions will need even more time to comply with the Proposed Guidelines. We urge the OCC to use the authority it reserved in the Proposed Guidelines to provide Banks new to the OCC's "heightened expectations" with an adequate implementation period, based on the current maturity level of the Bank's risk framework compared to the OCC's supervisory expectations and the Proposed Guidelines, but in any event at least one year from the date of the final rule.

Additional Areas of Clarification

The Associations recommend that several additional areas be revised to provide clarity to Banks regarding how examiners will review compliance with the Proposed Guidelines, and to ensure that the focus of resources and board time is appropriately placed on the most significant risks and emerging issues facing the Bank.

A. Requiring a single Chief Risk Executive for all Banks in all circumstances is too prescriptive for the varied risk profiles and organizational designs among Banks.

The Proposed Guidelines request comment on whether oversight of IRM should be consolidated under a single CRE. The Associations are opposed to such rigid requirements. Banks adopt organizational structures that are designed to address their particular risk profiles. For instance, some Banks may bifurcate responsibilities within IRM, based on the unique characteristics of the institution, and background of its risk management leadership team. The Bank's designated examination and supervision team is best able to assess whether the organizational design is appropriate based on the Bank's unique facts and circumstances, and can address the issues raised by a Bank's organizational structure in a tailored manner that better serves the Bank than through a single prescriptive approach.

B. "Substantially the Same" Test

We provide the following recommendations to clarify further when and how a Bank can avail itself of the "substantially the same" test. The Proposed Guidelines state that a Bank should conduct, at a minimum, an annual assessment to determine whether its risk profile is substantially the same as its parent's.[39] However, the Proposed Guidelines also state the measurement on which the test is based is determined using the most recent quarter-end Call Report.[40] The OCC should clarify that a Bank choosing to avail itself of the "substantially the same" test need only review the measurement criteria annually in connection with its annual assessment,[41] using the most recent Call Report data available.[42] The Associations also urge the

[38] *Id.* at 4283.
[39] *Id.* at 4297.
[40] *Id.*
[41] The Associations recognize that a reassessment should be conducted more frequently if circumstances result in a permanent change in the asset composition of the holding company or Bank, such as the acquisition of a significant nonbank subsidiary.

OCC to provide additional clarification that where a Bank meets the "substantially the same" test, the organization's risk management framework and governance, IRM and IA may be the same for the Bank and holding company if, through consultation with designated examination staff, this fact results in an effective risk management outcome for the Bank.

The Associations also recommend that Banks subject to the Proposed Guidelines be allowed to aggregate assets of multiple subsidiary national banks or Federal savings associations, in consultation with their designated examination staff, for purposes of determining whether they meet the "substantially the same" test. Some of the Banks subject to the Proposed Guidelines conduct banking activities in more than one bank charter for strategic and business reasons. Failure to allow institutions to aggregate Bank charters to meet the "substantially the same" test could result in forcing institutions to change strategic models in order to reduce the cost of duplicate risk management programs, which may not be in the best interest of their customers or communities. Finally, the OCC should also provide for a significant transition period if a Bank can no longer meet the criteria of the "substantially the same" test.

C. Foreign Banking Organizations

There are several foreign banking organizations (FBOs) that own subsidiary Banks that are subject to the Proposed Guidelines. However, it is unclear which parent company the OCC will look to in determining how a "parent company's" risk framework may be leveraged to meet the Proposed Guidelines or meet the "substantially the same" test. This is further complicated by the fact that the Federal Reserve recently issued its Final 165 Rule that requires FBOs with $50 billion or more of U.S. nonbranch assets to establish a U.S. Intermediate Holding Company (IHC) that is subject to certain risk management standards, including the establishment of a board risk committee that will oversee the risk framework in the United States, and a U.S. Chief Risk Officer. The Associations strongly urge the OCC to coordinate with the Federal Reserve to develop consistent rules applicable to FBOs in the United States. We recommend for purposes of the Proposed Guidelines, that the "parent company" of a Bank subsidiary of an FBO is the U.S. IHC required under the Final 165 Rule.[43]

D. Materiality

The Proposed Guidelines should modify the following requirements to incorporate for each a materiality standard: 1) that the Bank's written strategic plan includes a comprehensive risk assessment that analyzes risks that could impact the bank; [44] 2) IA's responsibility to report to the audit committee in writing, all conclusions and issues from audit work carried out including the identification of the root cause of any issue; [45] 3) the requirement for the Audit Committee to

---

[42] The Associations note that the Proposed Guidelines are silent as to what data should be used in determining the total average consolidated assets, off-balance sheet exposure, and assets under management of the holding company for purposes of the "substantially the same" test. The Associations recommend using the most recent FR Y- 9C for purposes of calculating the denominator under the test. In addition, the OCC should clarify how off-balance sheet exposure and assets under management are to be calculated using the Call Report and FR Y- 9C or reconsider using these two criteria entirely.

[43] If an IHC is not in place at the time of the effective date of the Proposed Guidelines, the OCC should look to the top tier U.S. bank holding company of an FBO Bank subsidiary.

[44] 79 Fed. Reg. at 4299 (II.D).

[45] *Id.* (II.C.3.c).

see all internal audit risk assessments;[46] and 4) the requirement that all changes to the audit plan be communicated to the Audit Committee.[47]

E. Strategic Plan

The Proposed Guidelines as currently written state that the CEO is responsible for the development of a written strategic plan. We ask that the Proposed Guidelines be revised to reflect that the CEO should be responsible for overseeing the development of the plan. Further, the Proposed Guidelines should clarify that IA's role in development of the strategic plan should be limited so as not to jeopardize the independence of the function. Finally, the requirement to have the strategic plan reviewed, updated, and approved should be limited to off-cycle material changes to the strategy of the Bank, rather than operating environment changes that are best addressed through operating and contingency plans.[48]

F. IRM Requirement to "Ensure"

The Proposed Guidelines state that IRM must ensure that Front Line Units comply with the Proposed Guidelines and that IRM should oversee the Bank's risk-taking activities.[49] Taken literally, the language could shift the ownership of risk within an institution from the business lines to risk management and require IRM to guarantee outcomes. The Proposed Guidelines should be revised to clarify that IRM is responsible for overseeing the development and implementation of a risk framework that is designed to comply with the Proposed Guidelines.

G. Risk Limits

The Proposed Guidelines state that Front Line Units are required to establish relevant risk and concentration limits,[50] but it is unclear how the business lines interact with IRM with respect to the establishment of those limits. Generally, the establishment and setting of risk limits, both Bank-wide and business level, is the responsibility of IRM. This is done to see that all limits within the Bank are consistent with the Bank's overall risk appetite and because IRM has the expertise and systems to establish and monitor the limits. In addition, as discussed in Section I.A. above, Bank specific risk limits are not managed in isolation from parent company risks. Rather, the measurement and monitoring of Bank risks, as well as the setting of risk limits, often feeds into the enterprise-wide governance framework. Business lines have input into the limits related to their areas of responsibility and must monitor their own compliance with relevant

[46] *Id.* at 4298 (I.C.5.i).
[47] *Id.*at 4299 (II.C.3.b).
[48] The Associations recognize that off-cycle revisions to strategic plans may be necessary in rare cases where a permanent change in the asset composition or strategy of a Bank occurs, such as could result from a significant acquisition.
[49] *Id.* at 4298 (II.C.2, II.C.2.e).
[50] *Id.* at 4299.

business level limits. The Associations request that the OCC clarify the relationship between Front Line Unit and IRM risk limit setting and monitoring responsibilities. In addition, the Associations seek clarification as to the extent that the Bank board is required to approve risk limits in connection with a risk appetite statement. Bank directors are not in the position to approve all of the granular limits that Banks have to manage risk. The Proposed Guidelines should be revised to require the board to be aware of the Bank's process for setting limits in connection with the risk appetite statement.

H. Risk Inventory

The Proposed Guidelines, as currently drafted, require IA to maintain a comprehensive and current inventory of the Bank's material businesses, products, services, and functions.[51] The OCC specifically asks whether IRM rather than IA should be responsible for maintaining the inventory. We note that in many Banks today business line units are responsible for initially providing an inventory of the businesses, products, and services they manage and develop, and IRM or IA then reviews and challenges the initial inventory developed by the business lines. IRM or IA is responsible for owning and maintaining the Bank-wide inventory. If IRM owns and maintains the inventory, IA then tests the completeness of the inventory. The Associations recommend that the Proposed Guidelines be revised to reflect: 1) that Banks should only be required to maintain one comprehensive inventory; 2) the involvement and responsibility of first line business units in the development of the inventory; and 3) that Banks should have flexibility in determining whether IRM or IA is responsible for owning and maintaining the inventory.[52]

I. Additional clarity is needed with respect to the relationship between the Proposed Guidelines and the "heightened expectations" supervisory program.

The OCC should clarify whether the Proposed Guidelines are intended to replace or supersede all previous correspondence and guidance from the OCC regarding the "heightened expectations" program, including previous examiner guidance. The OCC should also clarify how Bank examinations and evaluations will be modified once the guidelines are finalized. Under the "heightened expectations" program, Banks were rated as "Strong," "Satisfactory," or "Weak" related to the five "heightened expectations." The OCC should communicate clearly to Banks on how it intends to rate Bank risk management frameworks and governance once its Proposed Guidelines are finalized.

* * * * *

[51] *Id.* (II.C.3.a.)

[52] Many banking organizations maintain what might be better described as an "audit universe," which is built around activities and processes that should be subject to audit and which is generally not the equivalent to an inventory of every business, product, service, and function. The Proposed Guidelines should clarify that use of such an "audit universe" on which to base the Audit Plan would not be problematic as long as it is comprehensive and covers all material risks.

In conclusion, the Associations appreciate the opportunity to comment on the Proposed Guidelines and respectfully request consideration of the concerns and recommendations contained in this letter. We urge the OCC to revise the Proposed Guidelines to focus on the principles of effective risk management programs that can be tailored to each individual Bank's business model, risk profile, and complexity rather than overly rigid and prescriptive "one size fits all" requirements. We also request that the OCC provide clarity on the role of the Bank board in overseeing the Bank's risk program.

If you have any questions or need further information, please contact:

Beth Knickerbocker, Vice President and Senior Counsel, American Bankers Association at bknicker@aba.com or (202) 663-5042;

Richard Foster, Vice President and Senior Counsel for Legal and Regulatory Affairs, The Financial Services Roundtable at Richard.Foster@FSRoundtable.org or (202) 589-2424;

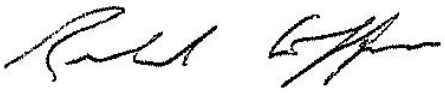
Richard Coffman, General Counsel, Institute of International Bankers at rcoffman@iib.org or (646) 213-1149; or

Carter McDowell, Managing Director and Associate General Counsel, Securities Industry and Financial Markets Association at cmcdowell@sifma.org or (202) 962-7327.

Sincerely,

Beth Knickerbocker
Vice President and Senior Counsel
American Bankers Association

Richard Foster, Vice President and Senior Counsel for Legal and Regulatory Affairs
The Financial Services Roundtable



Richard Coffman
General Counsel
Institute for International Bankers

Kenneth E. Bentsen, Jr.
President & CEO
Securities Industry and Financial Markets Association

Appendix A
Response to Specific OCC Questions

Question 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.

As discussed in Section I.A., the Associations strongly urge the OCC to reconsider its approach to compartmentalizing the Bank from its holding company risk management framework. That said, the Associations do appreciate that the OCC, through the "substantially same test," has permitted a very limited number of institutions to avoid the needless duplication of personnel, resources, and systems. However, as drafted, the "substantially the same test" fails to take into consideration value fluctuations and adjustments that may result in a Bank falling below the threshold temporarily, which could require Banks to build separate processes and systems, and hire personnel even though the Bank may still meet the spirit of what the OCC intended in creating the "substantially the same" test.

Question 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.

***See*, Section A- Additional Areas of Clarification.**

Question 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 Proposed 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.

***See*, Section G- Additional Areas of Clarification.**

Question 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?

***See*, Section I.D.**

Question 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?

The Associations do not oppose the OCC's requirement for two independent directors on the Bank board and believe that two is an appropriate number. However, as discussed in Section I.E., the Associations urge the OCC to coordinate with the Federal Reserve and adopt consistent regulations and supervisory expectations with respect to the risk governance structure of large financial institutions. The OCC should adopt a definition of "independence" that is consistent with the Federal Reserve's definition under Section 252.33(4) of the Final 165 Rule and the Securities and Exchange Commission Rule S-K.

Finally, as discussed in Section I.A., Banks should be permitted flexibility in meeting the requirements contained in the Proposed Guidelines by leveraging parent company board committees, including risk, compensation, and audit committees (which would be consistent with current OCC guidance and/or practice). As long as the Bank can demonstrate that risks to the Bank are effectively overseen through parent company board committees, we believe that requiring duplicate board committees at the Bank level is not necessary.

Appendix B
About the Associations

The American Bankers Association represents banks of all sizes and charters and is the voice of the nation's $14 trillion banking industry and its 2 million employees. Learn more at www.aba.com.

As *advocates for a strong financial future*™, The Financial Services Roundtable (FSR) represents 100 integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America's economic engine, accounting directly for $98.4 trillion in managed assets, $1.1 trillion in revenue, and 2.4 million jobs.

The Institute of International Bankers (IIB) is the only national association devoted exclusively to representing and advancing the interests of the international banking community in the United States. Its membership is comprised of internationally headquartered banking and financial institutions from over 35 countries around the world doing business in the United States.

The IIB's mission is to help resolve the many special legislative, regulatory, tax and compliance issues confronting internationally headquartered institutions that engage in banking, securities and other financial activities in the United States. Through its advocacy efforts the IIB seeks results that are consistent with the U.S. policy of national treatment and appropriately limit the extraterritorial application of U.S. laws to the global operations of its member institutions. For more information, visit www.iib.org.

The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to develop policies and practices which strengthen financial markets and which encourage capital availability, job creation and economic growth while building trust and confidence in the financial industry. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit www.sifma.org.