March 28, 2014

Office of the Comptroller of the Currency
400 7th Street SW., Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219
Attention: Legislative and Regulatory Activities Division
Docket ID OCC-2014-0001
RIN 1557-AD78

Re: 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 (Docket ID OCC-2014-0001)

Ladies & Gentlemen:

The Clearing House Association L.L.C. ("**The Clearing House**")[1] appreciates the opportunity to comment on the proposed guidelines issued by the Office of the Comptroller of the Currency ("**OCC**"), *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations* (the "**Proposed Guidelines**").[2] The Proposed Guidelines would establish minimum standards for the design and implementation of a separately identifiable risk governance framework for any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank with average total consolidated assets of $50 billion or more ("**Bank**").

The Clearing House strongly supports what we believe to be the fundamental goal of the Proposed Guidelines: a robust, identifiable risk management framework that identifies Bank-specific risks, manages those risks appropriately, and works closely with the enterprise-wide risk management framework of the holding company. Indeed, we believe the Proposed Guidelines are primarily intended to establish written standards that reflect and recognize the significant risk management improvements

[1] Established in 1853, The Clearing House is the oldest banking association and payments company in the United States. It is owned by the world's largest commercial banks, which collectively hold more than half of all U.S. deposits. The Clearing House Association L.L.C. is a nonpartisan advocacy organization representing – through regulatory comment letters, amicus briefs, and white papers – the interests of its owner banks on a variety of systemically important banking issues. Its affiliate, The Clearing House Payments Company L.L.C., provides payment, clearing, and settlement services to its member banks and other financial institutions, clearing almost $2 trillion daily and representing nearly half of the automated-clearing-house, funds-transfer, and check-image payments made in the United States. *See* The Clearing House's web page at www.theclearinghouse.org.

[2] 79 Fed. Reg. 4282 (January 27, 2014).

that Banks have already been implementing in response to more informal OCC supervisory communications over the last several years (the "**Heightened Expectations**"). In this respect, the Proposed Guidelines do not appear intended to be a significant departure from the Heightened Expectations that the OCC has previously communicated.

Nevertheless, we are very concerned that some of the particular language used in the Proposed Guidelines to codify the Heightened Expectations, if not clarified, could be interpreted to require very substantial – and we think unnecessary and ultimately counterproductive – changes to a Bank's risk management practices. While the language may not be intended to have such far-reaching effects, the concern that it could is real: ambiguities and lack of detail in some aspects of the Proposed Guidelines create the potential for unintended consequences, while other, very prescriptive requirements could represent a marked departure from the expectations that supervisors have previously communicated. These concerns are especially pronounced since the Proposed Guidelines, which are to be incorporated in Part 30 of the OCC's regulations, are expressly intended to facilitate the agency's ability to take enforcement actions when the Guidelines are breached.[3]

In particular, as described in more detail below, we have identified several key concerns with the Proposed Guidelines:

- **Uncertainty Relating to Ability to Share Risk Management Resources of the Consolidated Group.** There is real uncertainty about the degree to which a Bank's risk management framework may leverage robust aspects of enterprise-wide risk management of the Bank's parent holding company that are focused on the Bank – as is currently done – rather than separately re-creating and unnecessarily duplicating functions, personnel, and systems at the Bank level. If required, such duplication and "silo-ing" of the Bank's framework could make it more difficult for a consolidated group to achieve an enterprise-wide and cohesive approach to risk management as required under other guidelines or regulations.

- **Prescriptive Roles and Reporting Lines for Legal, Compliance and Other "Support Units".** The "three lines of defense" set forth in the Proposed Guidelines appear to introduce a new and highly prescriptive concept: non-revenue-generating units that engage in significant control activities, such as Legal, Human Resources ("**HR**"), Finance, Treasury, and Information Technology ("**IT**") – are now recast as "front line" units, without recognizing that the risks residing in these control functions are fundamentally different from the types of risks that exist in revenue-generating units and that a different degree of risk management oversight and flexibility would be appropriate for the control functions of such units.

- **Director Responsibilities that Appear to Blur the Distinction Between Oversight and Management.** Certain new requirements applicable to the board of directors of the Bank – especially that they "ensure" certain results – appear to blur the important line between the board's traditional and statutorily mandated oversight responsibility and managerial responsibilities that are appropriately the ambit of senior management. Other language could be interpreted as re-casting well understood fiduciary duties of Bank directors. Taken

[3] 79 Fed. Reg. at 4283-4284.

together, this proposed text could cause unintended consequences that may include deterring individuals from serving on a Bank's board.

- **Prescriptive Requirements and Reporting for Internal Audit.** The treatment of the internal audit function in the Proposed Guidelines deviates from well-established and sound practices that have been previously endorsed by the OCC and other standard-setters. For example, we are concerned that the Guidelines would preclude the Chief Audit Executive ("**CAE**") from administratively reporting to senior executives and that the Guidelines include prescriptive and burdensome requirements with respect to board oversight of internal audit and required benchmarking against leading industry practices.

The remainder of this letter provides additional details about these and other concerns and areas of ambiguity, and suggests modifications to address these concerns in the OCC's Final Guidelines. We believe that these suggested modifications would enhance the clarity of the Guidelines, create a more workable framework that is more closely in line with what we believe the OCC intended, and facilitate compliance – while still achieving the OCC's objective of achieving strong Bank-level risk management and active board oversight.

I. Relationship between Risk Management Frameworks of a Bank and its Parent Holding Company

We support the fundamental concept underlying the Proposed Guidelines that an effective risk management framework should be (i) capable of distinguishing, identifying, and monitoring aggregate risk at the Bank level, (ii) appropriately tailored to the Bank's risk profile, and (iii) designed to provide for robust checks and balances to ensure the integrity of the Bank's risk management process. In practice, such a framework under the Final Guidelines should permit a Bank's supervisors and examiners to identify the Bank's risk profile, risk appetite statement and risk limits, and to understand how the Bank meets the risk reporting requirements of the Guidelines.

Nevertheless, achieving these underlying objectives through a "separate bank risk management framework" should not mean that a Bank must recreate and duplicate at the Bank level components of the holding company's risk management framework that appropriately address distinct, Bank-specific risks, with separate personnel and reporting systems. Indeed, in complying with the OCC's Heightened Expectations to date, many Banks have successfully used "dual-hatted" personnel who perform risk management or related functions at both the holding company and the Bank, as well as Bank-oriented reporting systems and functions operated centrally at the holding company. In addition, where the holding company predominantly consists of national banking assets and activities, the need for distinct risk management frameworks for the Bank and the holding company is obviously diminished. Reduced to its core purpose, a risk framework, whether housed at the holding company or at the individual Bank or legal entity level, should provide a mechanism through which all covered businesses carry out specific routines to establish appropriate risk appetites, risk governance procedures, risk reporting routines and specific risk management processes to identify, measure, monitor, and respond to risks affecting both the individual business units and the enterprise as a whole.

Our concern is that the specific language of the Proposed Guidelines does not make sufficiently clear that the current practices involving overlaps of holding company and Bank risk management functions – which have been in many cases expressly adjusted to address the OCC's Heightened Expectations – would continue to be permissible. Clarification in this regard would

appropriately recognize that the underlying objectives of the OCC may be achieved where the risk management framework can separately measure and report risk at the Bank level even where there exists overlap with the enterprise-wide framework. Details regarding these concerns are set forth below, along with suggested modifications.

A. Bank Leverage of Holding Company Risk Management Framework and Personnel "Dual-Hatting"

The Final Guidelines should clarify that a robust holding company function that includes a distinct Bank component can be used to meet the OCC's risk management expectations at the Bank level. One example, deployed in many institutions, is a centralized internal audit function at the holding company that identifies Bank-specific risks. While Banks' reliance on this holding company function generally has been effective, and viewed by the OCC as consistent with the Heightened Expectations, it is not clear that it would remain permissible under the Proposed Guidelines. Similarly, many holding companies determine Bank-specific risk limits using a centralized management information system ("**MIS**") operated at the holding company level, with the Bank employing this holding company MIS as part of its own Bank-level risk management. Again, it is unclear whether such common MIS practices would be permissible under the Proposed Guidelines. While we do not believe that the intent of the OCC is to prohibit such practices, the Final Guidelines should expressly state that the above-mentioned examples and other instances of overlapping practices are permissible. Permitting such overlap would allow Banks to comply with the Guidelines in a more efficient and cost-effective manner, rather than having to duplicate functions at the Bank level.

In addition, many holding companies have established enterprise-wide functions to promote uniform and consistent internal controls that are designed to satisfy statutory or regulatory mandates that apply irrespective of the legal entity engaged in the activity; such enterprise-wide functions should be permissible when applied at the Bank level.[4]

Similarly, the Final Guidelines should expressly state that it is permissible for an individual to serve as a risk management employee of both the Bank and its holding company. Such "dual-hatting" practices are widespread, and they allow a Bank to tap the most qualified personnel at an organization to serve in key roles at the Bank, and provide for a more cohesive approach to enterprise-wide risk management for the consolidated banking organization. For example, in an era where there are significant sovereign risks facing global Banks, it is far better for a single group to consider the potential risks to the enterprise and the national Bank, and potential overlaps in those risks, rather than having a siloed approach.

Indeed, dual-hatting is especially important with respect to the roles of Chief Risk Executive ("**CRE**") and CAE, where it can be critical for the Bank to have direct access to the most

[4] *See*, *e.g.*, 12 C.F.R. Part 34, Subpart C; Board of Governors of the Federal Reserve System (the "**Federal Reserve**") *Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles*, SR 08-8 (October 16, 2008) (stating that larger, more complex institutions ". . . typically require a firmwide approach to compliance risk management and oversight that includes a corporate compliance function. . . . Firmwide compliance risk management refers to the processes established to manage compliance risk across an entire organization, both within and across business lines, support units, legal entities, and jurisdictions of operation. This approach ensures that compliance risk management is conducted in a context broader than would take place solely within individual business lines or legal entities.")

experienced personnel from its parent holding company. In addition, this dual-hatting allows the Bank's CRE and CAE to have an in-depth and hands-on understanding of the activities and risks of the Bank's parent holding company and nonbank affiliates, thereby better enabling the CRE and CAE to understand what impact those activities and risks may have on the Bank, and take action to limit such impact when appropriate.[5]

Additionally, for senior management positions in the risk and audit functions, there are significant benefits to having personnel with an enterprise-wide view, such as a deeper understanding of the overall organization, inter-affiliate relationships, and the broader technology environment of the entire organization. Banks and their holding companies have therefore been permitted to share such personnel where that practice effectively achieves risk management goals, including in the context of supervisory communications implementing the Heightened Expectations, as long as the interests of both the Bank and the holding company are appropriately considered (*i.e.*, the safety and soundness and the fiduciary duties to other entities). As a result, we suggest that the Final Guidelines expressly clarify that dual-hatting practices are permissible, including for the most senior risk management and internal audit personnel.

B. "Substantially the Same" Test

We strongly support the Proposed Guidelines' recognition that where the risk profile of the Bank and the holding company is "substantially the same," – *i.e.*, the predominant proportion of assets, activities, and risks of the holding company are housed in its banking subsidiaries – it is particularly justifiable for a Bank to share the holding company's risk management framework. Where the risk profiles of the different entities are so aligned, there appears to be little need to create separate risk management frameworks, and indeed, it would be far more effective and efficient to operate a single framework.

The Proposed Guidelines provide two avenues for a Bank to meet the "substantially the same" test:

- Where a Bank's average total consolidated assets, total assets under management, and total off-balance sheet exposures constitute 95 percent or more of those same balances of its parent company (the "**Objective Test**"); or

- For a Bank that does not satisfy the Objective Test, where it requests and receives a determination from the OCC that its risk profile is substantially the same as its parent's risk profile based on other factors (the "**Subjective Test**").

As described below, our essential concerns are that the Objective Test is too stringent, while for those Banks that cannot satisfy that test, the Subjective Test is too vague and uncertain.

[5] Indeed, permitting dual-hatting is wholly consistent with the objective set forth in the Proposed Guidelines that IRM and internal audit should attract and retain talent to effectively carry out their respective roles and responsibilities. 79 Fed. Reg. at 4298 (col. 2), 4299 (col. 1).

1. The Objective Test of 95 Percent Is Too Stringent and Should Be Set at 85 Percent

The Objective Test would effectively operate as a kind of "safe harbor." Where the 95 percent threshold is passed, a Bank would not need to establish a separate risk management framework from its holding company – so long as the holding company's framework satisfies the Guidelines and the Bank provides a documented assessment each year that it continues to meet the 95 percent test.[6]

While we support the concept of an objectively measured safe harbor for these purposes, we believe the 95 percent threshold is too stringent. Specifically, we believe that an 85 percent threshold is more appropriate. Where no more than 15 percent of the holding company's assets, assets under management, and off-balance-sheet exposures reside outside the Bank, the risk profile of the Bank can legitimately be said to be substantially the same as the holding company without further evidence of "sameness" – and to the extent there are significant differences in the risk profile resulting from assets and exposures in the 15 percent number, the OCC could require adjustments to the Bank's risk management framework on a case-by-case basis.

Moreover, an 85 percent threshold is consistent with other thresholds applied in analogous regulatory contexts. For example, under the regulations for resolution plans issued by the Federal Reserve and the Federal Deposit Insurance Corporation, a firm may elect to submit a "tailored" plan if it has less than $100 billion in total nonbank assets and its total insured depository institution assets are 85 percent or more of its total consolidated assets.[7] Likewise, the Federal Reserve has also adopted tests based on 85 percent of a company's total annual gross revenues and consolidated total assets to determine whether a company is "substantially engaged" in activities permissible for a financial holding company.[8]

---

[6] The Proposed Guidelines state, "[a] parent company's and Bank's risk profiles would be considered substantially the same if, as of the most recent quarter-end Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income (Call Report), the following conditions are met: (i) The Bank's average total consolidated assets represent 95% or more of the parent company's average total consolidated assets; (ii) the Bank's total assets under management represent 95% or more of the parent company's total assets under management; and (iii) the Bank's total off-balance sheet exposures represent 95% or more of the parent company's total off-balance sheet exposures." 79 Fed. Reg. at 4284 (col. 3). While the information for the numerator would be in the Call Report, the information for the denominator would be in the Federal Reserve Board's Form FR Y-9C, Consolidated Financial Statements for Holding Companies. The Clearing House supports the use of current regulatory reports for purposes of documenting that a Bank meets the Objective Test, but believes that the Final Guidelines should specify that this calculation may be based on both the Call Report and Form FR Y-9C, and should set forth how the OCC intends for Banks and their holding companies to calculate total assets under management and off-balance sheet exposures under the currently prepared regulatory reports. Indeed, in light of the limited information required to be reported on the FR Y-9C with respect to assets under management and, more generally, the relatively limited additional insight that such information would likely provide over that already offered by the total average consolidated assets and total off-balance sheet exposure prongs of the Objective Test, we submit that the OCC should reconsider the need to include assets under management as part of the Test. The size of assets under management without regard to the types of products offered and the complexity of the operation is not an accurate measure of risk.

[7] 12 C.F.R. §§243.4(a)(3), 381.4(a)(3); 76 Fed. Reg. 67,323, 67,336 (November 1, 2011).

[8] *See* 12 C.F.R. § 225.85(a)(3)(ii).

Regardless of the numerical threshold chosen, we believe that the Final Guidelines should make clear that the Objective Test should not be applied on an individual Bank basis. That is, where a holding company owns more than one Bank subsidiary, the test should not require that *each* subsidiary meet the 95 percent test separately (which would be mathematically impossible); instead, the banking organization should be allowed to aggregate the assets, assets under management, and off-balance sheet exposures of *all* the holding company's Bank subsidiaries for purposes of determining the numerator of the required ratio. For example, where a holding company has a large commercial bank and a large credit card national bank as its two principal subsidiaries – as often is the case – aggregation of the two subsidiaries' assets and exposures should be permitted for purposes of the Objective Test threshold. Such subsidiaries are often subject to a common risk management framework and, given the similarity of rules and requirements applicable to both, there appears to be little benefit in requiring two separate risk management frameworks. At the very least, there should be some kind of presumption articulated in the Final Guidelines that such Bank subsidiaries of a banking organization, even if they did not satisfy the Objective Test's safe harbor, would nevertheless be very likely to satisfy the Subjective Test for determining "substantial sameness."

2. The Subjective Test Should be Clarified

Under the Subjective Test, a Bank that fails to satisfy the Objective Test may nevertheless request a determination from the OCC that the risk profiles of the Bank and its holding company are substantially the same based on "other factors." Examples of such "other factors" are not described in either the Proposed Guidelines or its Preamble.

While we understand this logic, our concern is that without more detail or examples of such "other factors," the Subjective Test is so vague that it may apply extremely narrowly, even where a Bank's risk profile is very similar to its parent company's. We therefore believe that it would be very helpful for the Final Guidelines to include, at a minimum, examples of the types of circumstances under which the Subjective Test would likely be satisfied. For example, if the OCC declines to allow aggregation of banking assets in different Bank subsidiaries for purposes of determining compliance with the Objective Test, it ought to make clear that such aggregation might well be a deciding factor in determining compliance with the Subjective Test. In this regard, the OCC ought to take into account scenarios where a national bank charter may be held for an institution that performs very limited activities, such as a trust company, and therefore it may not be necessary or appropriate for the entity to have its own risk governance framework (but the existence of such an entity could potentially disqualify a large affiliated Bank under a strict application of the 95 percent test). Alternatively, a Bank may have a parent holding company that also owns an entity that is effectively no longer operating and is in a wind-down or sell-off stage. In such circumstances, it may be appropriate to exclude any such assets in calculating the parent's total assets for purposes of the 95 percent test calculations or to otherwise take such circumstances into account for purposes of administering the Subjective Test.

In addition, it would be helpful if the OCC provided further specificity and clarity regarding the process for determining whether the Subjective Test is satisfied. Given the likelihood that proprietary, commercially sensitive, and confidential supervisory information would be involved, we believe that such a process should be a confidential one, conducted by supervisors on an institution-by-institution basis; it should not be a public notice and comment process.

Moreover, for a Bank that is allowed to rely on the risk management framework of its parent holding company, the Final Guidelines should clarify expectations regarding the required annual

assessment of the substantial similarity of the two entities' risk profiles. We recommend that, after the initial assessment has been agreed to by the OCC, the agency allow subsequent annual assessments to be supplemental and iterative, rather than require full-blown "*de novo*" annual submissions. Such supplemental submissions would be far less burdensome while still achieving the objective of providing a robust process for determining that a Bank's risk profile remains substantially the same as its parent holding company's.

Finally, for a Bank whose risk profile no longer meets the "substantially the same" test, however that is determined, the Final Guidelines should include transitional provisions providing the Bank with adequate time to comply with the Guidelines on a standalone basis.

3. Application of "Substantially the Same" Test to FBOs

Bank subsidiaries of Foreign Banking Organizations ("**FBOs**")[9] subject to the Guidelines should have the flexibility under the "substantially the same" test to compare the subsidiary Bank's risk profile to its parent U.S. intermediate holding company ("**IHC**"), its ultimate FBO parent holding company, or any other holding company where the risk governance framework is housed within the organization. In particular, where the risk profiles of a Bank and its IHC parent (or any other parent holding company of the Bank) meet either the Objective Test or the Subjective Test, there is no compelling reason for the OCC to require a separate risk management framework for the Bank – the logic is the same as it would be for a Bank and its U.S. parent holding company where no foreign ownership is involved. Of course, that common risk framework of the Bank and its IHC (or any other parent holding company of the Bank) would still need to comply with the requirements of both the Guidelines and applicable Federal Reserve regulations.

C. Coordination with the Federal Reserve

The Proposed Guidelines would impose specific risk management requirements on Banks, while the Federal Reserve has imposed separate risk management requirements on large bank holding companies.[10] We strongly believe that the OCC and the Federal Reserve should coordinate their rulemaking and supervisory efforts to ensure that regulated institutions are subject to consistent risk management expectations; banking organizations should not be placed in the untenable position of having to reconcile conflicting regulatory mandates and requirements. In addition to coordinating risk management rules or guidelines, the OCC and the Federal Reserve should also coordinate the *implementation* of such requirements to ensure consistency and avoid needless conflict. We strongly recommend that the OCC consider the interplay between the Proposed Guidelines and the Federal

[9] *See* 12 C.F.R. § 211.21(o).

[10] *See, e.g.*, Federal Reserve, *Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations*, Docket No. 1438 (February 18, 2014); SR 08-8, *Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles* (October 16, 2008); SR 08-9, *Consolidated Supervision of Bank Holding Companies and the Combined U.S. Operations of Foreign Banking Organizations* (October 16, 2008). See*, supra*, note 4.

Reserve's separate risk management requirements and ensure that the OCC's framework remain flexible enough to enable a banking organization to comply with both sets of rules.[11]

II. Lines of Defense

We support the general risk management principle of a "three lines of defense" model: (i) the first line of defense consists of front-line business units that have responsibility for assessing, managing, and controlling risks originating from their activities; (ii) the second line of defense consists of those units or functions that focus on measuring, managing, or controlling risks, including overseeing controls used by the first line of defense to mitigate and manage risks; and (iii) the third of line of defense is internal audit, which engages in independent testing of and assurance on the entire governance, risk management and control framework. While the Proposed Guidelines embrace the concept of three lines of defense, in doing so they introduce a new concept that is very different from the way that many institutions organize their risk management functions; significantly deviates from regulatory guidance issued by other regulators discussing the three lines of defense; is potentially very problematic; and will likely result in unintended consequences.

Specifically, the Proposed Guidelines assign Independent Risk Management ("**IRM**") to the second line of defense; all other units (except internal audit) are treated exclusively as front-line units in the first line of defense, including units that engage in significant control functions, such as Legal, Finance (including the Comptroller), Treasury, IT, and HR. (The Proposed Guidelines do not specify where Compliance would fall within the three lines of defense.) As a result, units or parts of units engaged in control functions would be subjected to the very same requirements as revenue-generating business units, with no recognition that these units are principally managers, rather than generators, of risk. Further, IRM is charged under the Proposed Guidelines with "ensuring" that all front-line units comply with the risk management standards they establish for themselves or that IRM establishes for them. As a practical matter, this would likely make units engaged in control activities subordinate to IRM in fundamental and problematic ways.

In short, this change in the Proposed Guidelines could force Banks to significantly modify their organizational structures, reporting lines, and risk control practices through a "one-size-fits-all" approach that could impair Banks' ability to effectively manage risks. Again, while this may not be the intent of the Proposed Guidelines, our very real concern is that it could have this effect. We believe the proposed modifications discussed below would better capture current and sound industry practices for risk management frameworks, and would do so in a manner that is fully consistent with the Heightened Expectations.

---

[11] *See, e.g.*, remarks by Thomas J. Curry, Comptroller of the Currency, 49th Annual Conference on Bank Structure and Competition (May 9, 2013) ("Toward that end, we are also stepping up our coordination with other agencies, including the Fed, the FDIC, and the CFPB, to develop integrated strategies for joint supervision of complex institutions and new tools to aid oversight. This process involves the sharing of information, but it's much more than that. In a world of increasingly complex financial institutions, we need to be able to allocate supervisory resources more effectively and take advantage of each other's work. As Comptroller, I have made interagency collaboration one of my top priorities.")

A. In General, Control Units Should Be Included in the Second Line of Defense

We believe that units that are fundamentally engaged in control activities ought to be included in the second line of defense, not the first line of defense. Such units, including Legal and Compliance, analyze risks through a different lens than IRM. In order to take advantage of the various inputs on the risks of business activities, control units need to operate independently and not have their perspectives actually or functionally subordinated to IRM. In contrast, the Proposed Guidelines, by treating all non-revenue-generating units as front-line units in exactly the same manner as revenue-generating units, and by requiring IRM to oversee all the risks of such units and to ensure that they comply with all applicable risk management standards, could have the effect of shifting a significant amount of responsibility for control units to IRM. Indeed, they could very well require IRM to oversee substantive activities of these units.

This creates a number of concerns and questions. For example, is it intended that substantive legal advice of Legal, such as opining on attorney/client privilege issues, will be subject to review and second-guessing by IRM? Likewise, should advice by accountants regarding interpretations of Generally Accepted Accounting Principles be subject to IRM review? Should IRM oversee the ability of IT to monitor compliance with its technical policies by other business units? Is it intended that Legal and Compliance report to or be overseen by IRM?

If the answers to these questions are "yes," that would constitute a very substantial change to the way that most banking organizations currently conduct their control and risk management functions. It would also constitute a marked departure from our understanding of the types of risk management practices, reporting lines, and control activities that have been acceptable for purposes of the Heightened Expectations previously communicated to Banks. More fundamentally, such a change could require all Banks to adhere to an identical reporting framework, which in many cases would not be advisable – especially since IRM is simply not structured to second-guess the substantive control advice provided by Legal, Compliance, Finance, or other units engaged in control functions.

But if the answers to these questions are "no," as we hope and expect is the case, then we strongly recommend the OCC realign the three lines of defense as described below. In particular, it is critical that the Final Guidelines appropriately recognize that *all* control units, not just IRM, help to ensure that risks in the business units have been appropriately identified and managed, with the result that they would be treated as second-line units. Indeed, this result would be fully consistent with standards expressly articulated by international standard-setting bodies, where units with significant control functions, including Legal, Compliance, HR, IT, and Finance, are grouped with risk management as second lines of defense.[12]

[12] Different approaches have been taken (or terminology used) by supervisors and banks in drawing the line between second line of defense internal controls and risk management. *See, e.g.*, Basel Committee on Banking Supervision (the "**Basel Committee**"), *Principles for Enhancing Corporate Governance*, n. 23 (October 2010) ("While risk management and internal controls are discussed separately in this document, some supervisors or banks may use "internal controls" as an umbrella term to include risk management, internal audit, compliance, etc. The two terms are in fact closely related and where the boundary lies between risk management and internal controls is less important than achieving, in practice, the objectives of each.")

For example, in a 2012 paper, the Basel Committee stated that "[t]he business units are the first line of defence. They undertake risks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks of their business. The second line of defence includes the support functions, such as risk management, compliance, legal, human resources, finance, operations, and technology."[13] The Committee of Sponsoring Organizations of the Treadway Commission's ("**COSO**") Internal Control Integrated Framework embraces the same conclusion: "Business-enabling functions such as risk, control, legal, and compliance provide the second line of defense as they clarify internal control requirements and evaluate adherence to defined standards. While they are functionally aligned to the business, their compensation is not directly tied to performance of the area to which they render expert advice."[14] Finally, the Financial Stability Board (the "**FSB**") has observed, "[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 groups with sufficient expertise in these areas, such as Information Security, Privacy, Technology Risk Management, Corporate Security, Business Continuity, Compliance etc."[15]

B. Legal and Compliance Should Be Included in the Second Line of Defense

Legal and Compliance are both units whose fundamental purpose is to engage in a control function. While some lawyers and compliance personnel work closely with front-line business units, that does not change the control character of their activities.

For example, Legal plays a vital role in protecting and serving the Bank as a whole, not any particular business unit, even if individual lawyers may be assigned to assist specific business units. The duty of a Bank's legal department is to protect the Bank, not the business. While certain members of Legal may work closely with a specific business unit, advising the business whether its activities are in compliance with law, Legal's ultimate responsibility is the overall protection of the Bank. Additionally, various standards apply to counsel that serve to promote the independence of the function, including, among others, Sarbanes-Oxley "Up the Ladder" reporting requirements,[16] and Ethical Codes applicable to attorneys in connection with their licensure to practice law in particular jurisdictions.[17] Thus, the Final Guidelines should clarify explicitly that Legal is in the second line of defense.

---

[13] Basel Committee, *The Internal Audit Function in Banks*, at 12-13 (June 2012).

[14] COSO, *Internal Control – Integrated Framework*, at 147 (May 2013).

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

[16] Section 307 of the Sarbanes-Oxley Act of 2002 (requiring attorneys to report evidence of a material violation by an issuer to the issuer's Chief Legal Officer and Chief Executive Officer or Audit Committee); 12 C.F.R. § 205 *et. seq.*

[17] *See, e.g.*, New York State Unified Court System, Part 1200, Rules of Professional Conduct, Rule 5.8(a): "The practice of law has an essential tradition of complete independence and uncompromised loyalty to those it serves. Recognizing this tradition, clients of lawyers practicing in New York State are guaranteed 'independent professional judgment and undivided loyalty uncompromised by conflicts of interest.' Indeed, these guarantees represent the very foundation of the profession and allow and foster its continued role as protector of the system of law. Therefore, a lawyer must remain completely responsible for his or her own independent professional judgment . . . and otherwise comply with the legal and ethical principles governing lawyers in New York State."

Likewise, Compliance plays a crucial role in helping front-line units conduct their activities in a manner that complies with law and regulation – a classic control function. While the Proposed Guidelines are virtually silent about the intended treatment of Compliance in the three lines of defense, we believe the Final Guidelines should clarify that it is squarely in the second line, even with respect to those personnel that work closely with front-line units. As described above, this is consistent with the approach of COSO, the FSB and the Basel Committee. We do not believe that a close working relationship between Compliance and front-line units compromise Compliance's independence. Indeed, in April 2005, the Basel Committee acknowledged that the need to maintain independence of the Compliance function is consistent with a close working relationship with front-line units:

> The concept of independence does not mean that the compliance function cannot work closely with management and staff in the various business units. Indeed, a co-operative working relationship between the compliance functions and business units should help to identify and manage compliance risks at an early stage. Rather the various elements described below should be viewed as safeguards to help ensure the effectiveness of the compliance function, notwithstanding the close working relationship between the compliance function and the business units. The way in which the safeguards are implemented will depend to some extent on the specific responsibilities of individual compliance function staff.[18]

In sum, given their core control functions, we believe both Legal and Compliance should be treated as second-line units. This is not to say that there could never be circumstances in which lawyers or compliance personnel could play more of a front-line function. Such circumstances would be the exception to the rule, and could be addressed by Banks and their supervisors on a case-by-case basis.

Similarly, although both Legal and Compliance are independent sources of control, we recognize that they can at times present certain types of operational risk – as is also true for IRM and internal audit. This factor alone, however, should not result in Legal and Compliance being treated as front-line units. In order to carry out its overall risk management responsibilities, we would expect IRM to continue to interact with Legal, Compliance, and many other units of the Bank other than the front-line revenue-generating units. Indeed, it is critical that IRM understand key risks, so the CRE may explain such risks to senior management and the board of directors.

C. Other Units with Both Control and Front-Line Functions Should Be Recognized in Both the First and Second Lines of Defense

Other units classified in the Proposed Guidelines as front-line – Finance, Treasury, HR, and IT – engage in both substantial control functions as well as operational functions unrelated to their role as a control function. For example, Finance may play a role in deciding the types of risk a Bank is willing to assume in funding itself, while also playing a very important control function in the Sarbanes-Oxley certification process. Similarly, HR may design compensation policies to encourage the right risk-balancing approach, but also oversee the implementation of its compensation policies – a control function – to make sure business units comply with them.

---

[18] Basel Committee, *Compliance and the Compliance Function of Banks*, Paragraph 20 (April 2005).

Given the important control functions of these units, we believe it would be inappropriate to classify such hybrid units as wholly front-line, as is the case with the Proposed Guidelines. Indeed, if one line were to be chosen for such units, it ought to be the second line, consistent with the approach of COSO, the FSB and the Basel Committee, as previously described. Another plausible approach would be to assign parts of such units to the first line, and parts to the second line, depending on their functions. The Final Guidelines should preserve flexibility for the classification of these other units within the three lines of defense to be made on an institution-by-institution basis subject to OCC review as part of the supervisory process.

As with Legal and Compliance, however, we would expect that IRM would engage in the oversight of operational risk for such units, even the parts that engage in control functions. But regardless of which line of defense these units are in, it would be problematic to subject such parts to the array of IRM requirements that would apply more generally to front-line units.[19]

D. Organizational Reporting Requirements for Legal, Compliance, and Other Units with Control Functions

The Final Guidelines should make clear that, regardless of the line of defense in which they are placed, Legal, Compliance, and other units with control functions are not required to organizationally report to IRM. Moreover, the Preamble to the Proposed Guidelines provides that "no front line unit executive oversees any independent risk management units."[20] To the extent a unit other than IRM is recognized in the second line as well, there is a concern that a similar restriction would apply, and which could cause unnecessary and unproductive changes to existing reporting lines that have not previously been questioned in the context of the Heightened Expectations. For example, if Compliance were treated as second-line and Legal – inappropriately – treated as front-line, then the Guidelines might be read to prohibit the Compliance from reporting to the General Counsel – even though that reporting relationship has been adopted and permitted for many Banks for many years.

We believe there should be flexibility in the Final Guidelines, as there is today, to allow such units with control functions to report to other units in the Bank, such as Compliance reporting to Legal, or Legal reporting to the Chief Executive Officer ("**CEO**"), and for such units to have their own internal reporting structures. This flexible approach would recognize that Legal, Compliance, and other control function structures, reporting lines, and practices vary across Banks due to differences in size, complexity, business model, and other factors. Bank reporting practices have generally reflected efforts to utilize resources and expertise in a manner that bolsters the effectiveness of the three lines of defense framework given the institution's unique characteristics.

E. Expectations for Control Functions Require Greater Flexibility

At a minimum, if the Final Guidelines continue to treat units engaged in control functions as exclusively front-line, they should expressly clarify that a "one size fits all approach" does

---

[19] *See* Basel Committee, *Principles for Enhancing Corporate Governance*, n. 24 (October 2010) ("While the design and execution of a bank's capital planning process may primarily be the responsibility of the chief financial officer, the treasury function, or other entities within the bank, the risk management function should be able to explain clearly and monitor on an ongoing basis the bank's capital and liquidity position and strategy.")

[20] *See, e.g.*, 79 Fed. Reg. at 4287 (col. 1).

not apply to the risk-management requirements for such units. Specifically, some requirements that apply to revenue-generating units, like risk and concentration limits, would not apply to support units like Legal, HR, and IT. As a result, the Final Guidelines should expressly state that the policies, procedures, and processes of front-line units should be tailored to the actual risks they face (*e.g.*, operational risk for IT, but not credit risk). They should also expressly state that not all units will be subject to specific risk limits so long as aggregate risks can be accurately assessed at the Bank level. As the risk affecting units engaged in control functions are primarily operational or reputational in nature, any risk-management requirements with respect to such units should appropriately focus on such risks. These may include, for example, reporting and risk indicators (to inform the CRE's overarching assessment of Bank risk) with respect to: (i) talent retention for HR, (ii) significant defensive litigation risk for Legal, and (iii) high impact information security events and availability of core platform applications for IT.

Similarly, if non-revenue-generating units continue to be treated as front-line units, we believe that it is important that the OCC provide greater detail about the expected relationship of these units to IRM, *e.g.*, to clarify that IRM's risk oversight function should not extend to independently assessing the risks imposed by litigation involving the Bank, or second-guessing substantive policies of Legal or IT, where IRM's expertise would be limited. Indeed, the Final Guidelines should clarify with specificity how IRM would in fact interact with non-revenue-generating front-line units as a practical matter, and how those expectations would differ from IRM expectations with respect to revenue-generating units.

Again, a far preferable solution to avoid these unintended consequences would be to modify the three lines of defense as discussed above in Part II.A-D.

F. The Role of the CEO with Respect to Independent Risk Management

Under the Proposed Guidelines, "Independent risk management should oversee the bank's risk-taking activities and assess risks and issues independent of the Chief Executive Officer and front line units."[21] In addition, however, under the Proposed Guidelines, the CRE reports to the CEO and the CEO is ultimately responsible for the Bank. The Final Guidelines should clarify that although the CRE is responsible for overseeing and assessing the Bank's risk-taking activities, the CRE is still subject to CEO oversight with respect to those activities.

G. The Proposed Guidelines Transfer Certain Independent Risk Management Responsibilities to the Front-Line Units Contrary to Sound Risk Management Practice

Under the Proposed Guidelines, primary responsibility for the design of a comprehensive risk governance framework is assigned to IRM. Roles and responsibilities with respect to the establishment of front-line unit risk limits as well as the ongoing identification, assessment, measurement and monitoring of risks to the Bank appear to be assigned to the front-line units. In order to properly manage risk on a Bank-wide basis, IRM must have an integrated view of aggregate and individual risks to the Bank.[22] While we do not think the OCC intended to prohibit IRM from having a

[21] 79 Fed. Reg. at 4298 (col. 2).

[22] In addition, as more fully discussed in Part I, Bank-level risks can be more effectively managed by taking into account the banking group's risk profile.

role in the establishment and management of front-line unit risk limits, the Proposed Guidelines could be interpreted as suggesting that the front-line units have exclusive responsibility for front-line risk limits.

The Proposed Guidelines delineate two classes of risk: (1) risks associated with front-line unit activities; and (2) Bank-wide aggregate risks. Front-line units are broadly responsible for "assessing and effectively managing all of the risks associated with their activities" on an ongoing basis.[23] In executing this responsibility, front-line units must "[e]stablish and adhere to a set of written policies that include front line unit risk limits…[s]uch policies should ensure risks associated with the front line unit's activities are effectively identified, measured, monitored, and controlled, consistent with the bank's risk appetite statement, concentration risk limits, and all policies established within the risk governance framework."[23] IRM, by contrast, is responsible for identifying and assessing material aggregate risks to the Bank on an ongoing basis. In so doing, IRM must "[e]stablish and adhere to enterprise policies that include concentration risk limits. Such policies should ensure that aggregate risks within the bank are effectively identified, measured, monitored, and controlled, consistent with the bank's risk appetite statement and all policies and processes established within the risk governance framework…."[24]

We firmly support the premise that front-line units own the risks associated with their activities. However, for many Banks, the experience required to perform the front-line risk roles and responsibilities set out in the Proposed Guidelines – and especially setting risk limits – resides today primarily within IRM. While each Bank manages risk in accordance with its size, complexity, and unique risk profile, whether controlling for credit, market, country, interest rate, liquidity, operational or other types of risk, the risk assessment process as well as the measurement, setting, and/or monitoring of risk limits applicable to front-line (risk-taking) units are often the primary responsibility of the IRM function. There are several reasons that Banks may choose to conduct their risk management in this manner. Notably, in some institutions IRM is organized such that it has the exclusive expertise to perform these roles and it owns the systems used to monitor individual front-line unit risks.

For these institutions, moving these functions to the front-line could require a substantial overhaul of systems, personnel, reporting lines, etc. with no clear benefit over existing practice. In addition, such a full-scale restructuring of risk management practice could result in unnecessary duplication of efforts given IRM's continuing need to have a full view of macro and micro risks to the institution in order to properly design, implement, and update the Bank's comprehensive risk governance framework.

Accordingly, we believe the Final Guidelines should expressly clarify that establishing and reporting on front-line risk limits is not necessarily the exclusive responsibility of the front-line units, and depending on each Bank's risk governance operating model, may also be performed by or in conjunction with IRM.

---

[23] 79 Fed. Reg. at 4298 (col. 2).

[23] *Id.*

[24] *Id.* (col. 3).

III. Board of Directors

In general, we believe that the standards established in the Proposed Guidelines for directors are appropriate. There are, however, several important instances where we believe the language unnecessarily (and perhaps inadvertently) exposes directors to significant additional legal liability. In other instances, the Proposed Guidelines are overly prescriptive and could have the effect of inappropriately causing directors to engage in management activities rather than oversight. Finally, there are instances in which additional clarification of intent would be welcome. These concerns are set forth in more detail below.

A. Requirement to "Ensure" an Effective Risk Governance Framework

The Guidelines provide that a Bank's board must "ensure" that the Bank establishes and implements an effective risk governance framework that complies with the requirements of the Guidelines.[24] The term "ensure" might be understood to imply that the board will need to be deeply involved in the day-to-day activities of the Bank, thereby transforming a board's core oversight function into a management function. The term also connotes a guarantee of results, in this case a guarantee that the Bank will have an effective risk governance framework that complies with the legally enforceable Guidelines. That in turn would imply that directors could be held liable for management actions even where the directors' oversight has been reasonable. While such a "strict liability" standard may not be intended, the very real concern is that use of the word "ensure" could lead to such a result.[25] As a 2013 report of the Group of Thirty noted, regulatory standards applicable to board oversight:

> [need] 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…[26]

To avoid any unintended consequences, the Final Guidelines should delete the term "ensure" and instead hew to the directors' core oversight function. Thus, rather than providing that "the board of directors should *ensure* that the bank establishes and implements an effective risk governance framework that meets the minimum standards described in these Guidelines," the Final Guidelines should instead provide that "the board of directors should *actively oversee* the bank's establishment and implementation of an effective risk governance framework that meets the minimum standards described in these Guidelines."[27] (Emphasis added.) This use of the term "actively oversee" would eliminate any notion of strict liability or guaranteed results. It would also more accurately reflect the oversight function that is the core of a director's duties. In addition, "active oversight" is the very term that the Guidelines appropriately use in the next paragraph.[28] And the requirement that the

---

[24] 79 Fed. Reg. at 4300 (col. 1).

[25] *See, e.g.*, Group of Thirty, *A New Paradigm: Financial Institution Boards and Supervisors*, at 28 (October 2013).

[26] *Id.*

[27] 79 Fed. Reg. at 4291 (col. 1).

[28] *Id*.

oversight be "active" connotes the type of constructive engagement or "credible challenge" that the OCC has consistently referenced as a cornerstone of its Heightened Expectations.

B. Potential Change in Fiduciary Duty of Bank Directors

Under general principles of corporate law, directors are required to act as fiduciaries subject to the duties of care and loyalty. Certain language in the Preamble and text of the Proposed Guidelines could be read to create an additional fiduciary duty for Bank directors. This would run counter to well-established standards of corporate law and potentially expose directors to third party actions for any alleged breach of such duty. In addressing the OCC's prior guidance on Heightened Expectations, the Preamble states, "[t]he first expectation, often referred to as preserving the sanctity of the charter, maintains 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."[29] While the language of the Proposed Guidelines does not refer to a "fiduciary" duty, the Proposed Guidelines state that "[e]ach member of the bank's board of directors has a duty to oversee the bank's compliance with safe and sound banking practices" and that "the board of directors should ensure that the bank establishes and implements an effective risk governance framework that meets the minimum standards described in the Guidelines."[30]

Our members recognize that the duty of care applicable to Bank directors includes an obligation to actively oversee the safe and sound operation of the Bank. However, we are concerned about the potential establishment of a new fiduciary duty and the associated exposure to liability this would create for directors, a result we do not believe the OCC intended. Such a result could make it even more difficult for banks to attract qualified candidates to serve on their boards. In order to avoid any possible confusion in this regard, use of the term "fiduciary" in the Final Guidelines should be limited to descriptions of the long-established duties of care and loyalty and the obligations that attend thereto.

C. Potential Change in Fiduciary Duty of an Independent Director of the Holding Company Who Also Serves as Independent Director of the Bank

The Preamble to the Proposed Guidelines states that "[t]o the extent the Bank's independent directors are also members of the parent company's board, the OCC expects that such directors would consider the safety and soundness of the Bank in decisions made by the parent company that impact the Bank's risk profile."[31] Although the OCC's jurisdiction is focused on Banks, and not their holding companies, this language could reasonably be read to alter the fiduciary duty applicable to a person when acting as a holding company director.

While requiring a person serving as an independent director of the holding company to consider the safety and soundness of the Bank sounds like an innocuous requirement, the language is vague, and the concern is that a holding company director could be second-guessed (and sued) whenever any action of the holding company could somehow be connected to a loss to or adverse effect on the Bank. No such fiduciary duty exists now for a holding company director and, to the extent the

[29] 79 Fed. Reg. at 4283 (col. 1).

[30] 79 Fed. Reg. at 4300 (col. 2).

[31] 79 Fed. Reg. at 4291 (col. 2).

language in the Proposed Guidelines were found to create one, it could create a powerful disincentive for an independent director of the holding company to also serve as an independent director of the Bank (thereby avoiding the new standard). Such a result appears at odds with the intent of the Proposed Guidelines, which expressly contemplate that a person could serve as an independent director of both the Bank and its holding company. Indeed, given the difficulty in attracting qualified directors to the boards of financial institutions, we recommend that the Final Guidelines avoid using the language that has caused this concern and the potential for deterring qualified directors.

This is not to say that concerns cannot arise when the same person serves as a director of both the Bank and its holding company. Indeed, the OCC has expressly addressed such concerns in prior guidance, but in language that is much more carefully crafted, to create no change to existing fiduciary duties of either a Bank or its holding company:

> A director who serves on the board of both a bank and its holding company must comply with the director's fiduciary duties to the bank, including the duty of loyalty. This duty bars conflicts of interest that may arise when actions that are in the best interest of the holding company conflict with those that are in the best interest of the bank.[32]

As this excerpt makes clear, the primary concern with the service of independent directors on both boards is the potential for conflicts of interest, a legitimate concern which ties to well-established corporate governance principles. As a result, we recommend that the OCC clarify in the Final Guidelines, consistent with its prior guidance, that an independent director of both a Bank and its holding company is expected to comply with his or her fiduciary duty to the Bank in the face of conflicts of interest with the holding company. Furthermore, to resolve any remaining ambiguity on this point, the Preamble to the Final Guidelines should expressly state that the Guidelines are not intended to establish or alter any fiduciary duty applicable to a holding company director.

In addition, the Dodd-Frank Act codified the Federal Reserve's longstanding expectation that a holding company will serve as a "source of strength" to its depository institution subsidiaries.[33] A director of a holding company must now take this new federal statutory requirement into account as part of his or her oversight function. Therefore, this new "source-of-strength" requirement should help ensure the safety and soundness of a holding company's subsidiary Bank.

D. Prescriptive Board Involvement in Hiring Decisions

With respect to human resources, the Proposed Guidelines would require the board or a board committee to hire the CEO, one or more CREs, and the CAE; approve the hiring of the direct reports of the CEO that have the skills and abilities to design and implement an effective risk governance framework; establish reliable succession plans for the individuals described above; and oversee the talent development, recruitment, and succession processes for (1) individuals two levels down from the CEO; (2) IRM; and (3) internal audit.

---

[32] OCC, *The Director's Book*, at 26 (October 2010).

[33] *See* 12 U.S.C. § 1831o-1.

This set of responsibilities is unusually prescriptive, especially the provisions requiring establishment of reliable succession plans for direct reports of the CEO and oversight of the talent development, recruitment, and succession processes for the individuals noted above. While we believe it may be appropriate for a board or a board committee to approve the hiring of certain direct reports of the CEO, establishment of reliable succession plans for such individuals and the oversight of talent development, recruitment, and succession processes for individuals two levels down from the CEO, for IRM, and for internal audit should be left up to the management of the Bank.

E. Whether the Guidelines Should Require More Independent Directors and/or Specific Board Committees

The Proposed Guidelines require that two members of the board be independent directors and, as described above, they expressly recognize that an independent director of the parent holding company's board may serve as an independent director of the Bank's board. The Proposed Guidelines do not require the Bank's board to form any specific committee (although they do imply that the Bank's board would have an audit committee); it appears to be contemplated that the Bank's board could leverage the work of committees of the holding company's board. The Preamble requests comment on whether these requirements are adequate to provide effective oversight of the Bank; whether two is the right number of independent directors; and whether the Bank should be required to establish particular committees, such as a risk committee or other committees, rather than leveraging the work of holding company board committees.

We believe that the new requirements in this regard are appropriate. Requiring two independent directors is a significant change from past practice that will, with respect to some institutions, certainly introduce a real measure of independence to a Bank's board. In this regard, we believe it is very wise to allow overlap with independent directors of the holding company, to help ensure both that independent directors with knowledge of the company as a whole are in a position to oversee the Bank, and that the most qualified individuals in a scarce pool of qualified directors are available to provide such oversight.

At the same time, there is no need to require more than two independent directors. As a wholly owned subsidiary of the holding company, which itself has independent directors, sound governance may be achieved where a majority of directors with clear knowledge about the operations of the Bank are in a position to provide effective director oversight.

Similarly, we believe there is no reason to require the board of the Bank to establish particular committees instead of leveraging the work of committees of the parent holding company's board. Since much of the work of the parent company's board committees focuses on the Bank, it would be redundant and costly to require an additional layer of oversight at every Bank. While some Banks may prefer to have such committees, that should be a judgment left to individual institutions; it should not be mandated for all Banks.

IV. Internal Audit

The Clearing House supports a robust internal audit function as the third line of defense in a Bank's risk management framework. We do, however, have some concerns about several parts of the Proposed Guidelines that address this function.

A. Reporting Line of Chief Audit Executive

We believe the OCC intended in the Proposed Guidelines to define the internal audit function consistently with existing OCC guidance, well-established industry practices, and Federal Reserve guidance. However, the Proposed Guidelines depart materially from the Comptroller's Handbook: Internal and External Audits (the "**OCC's Audit Handbook**"),[34] guidance from the Institute of Internal Auditors ("**IIA**"), and Federal Reserve guidance with regard to the reporting line of the CAE. We recommend that the OCC clarify the definition of "Internal Audit" to ensure appropriate consistency. Specifically, although the Proposed Guidelines provide for the CEO or audit committee to oversee the CAE, they do not provide for reporting flexibility to another senior executive, like the General Counsel for instance, on day-to-day administrative issues. Further, in declaring that Legal is a "first line unit," the Proposed Guidelines would appear to prohibit reporting from the CAE to the General Counsel since a requirement of the Guidelines is that "[n]o front line unit executive oversees internal audit."[35]

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 influence the auditor's work."[36] In addition, the OCC's Audit Handbook specifically references the IIA, a leading internal audit professional association, with regard to oversight and structure of the internal audit function.[37] The IIA's position, which is well-established, also recognizes a flexible reporting structure by providing 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."[38]

Finally, the Federal Reserve continues to enhance its supervisory focus on large complex financial institutions and holding companies. Specifically, in Supervisory Letter 13-1 ("**SR Letter 13-1**") the Federal Reserve acknowledges that "[a] reporting arrangement may be used in which the CAE is functionally accountable and report directly to the audit committee on internal audit matters (that is, the audit plan, audit findings, and the CAE's job performance and compensation) and reports administratively to another senior member of management who is not responsible for operational activities reviewed by internal audit."[39] SR Letter 13-1 further requires that "[i]f the CAE reports

---

[34] OCC's Audit Handbook (April 2003).

[35] 79 Fed. Reg. at 4288 (col. 1).

[36] OCC's Audit Handbook, at 23 (April 2003).

[37] *Id.* at 13.

[38] IIA, *International Standards for the Professional Practice of Internal Auditing*, Standard 1110 - Organizational Independence.

[39] Federal Reserve, *Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing*, SR 13-1/CA13-1 (January 23, 2013).

administratively to someone other than the CEO, the audit committee should document its rationale for this reporting structure, including mitigating controls available for situations that could adversely impact the objectivity of the CAE. In such instances, the audit committee should periodically (at least annually) evaluate whether the CAE is impartial and not unduly influenced by the administrative reporting line arrangement."[40]

The Clearing House supports the OCC's goal to require Banks to maintain a strong internal audit function, but urges the OCC to reconsider the Proposed Guidelines' "one-size-fits-all" reporting structure; when proper controls exist, alternative senior management reporting will allow the same intended independence and unfettered access to the board.

B. Need for Materiality Standard Applicable to Audit Reports

The Proposed Guidelines provide that internal audit must report to the board's audit committee conclusions, issues, and recommendations from audit work… "[that] should identify the root cause of *any* issue. . . ."[41] (Emphasis added.) While we support the objective of providing internal audit with clear reporting responsibilities to provide the audit committee with sufficient information, the language quoted above suggests that internal audit must provide reports regardless of the materiality of the identified issues. The Proposed Guidelines also state that the audit committee "reviews and approves internal audit's charter, *risk assessments*, and audit plans."[42] Read literally, these requirements risk inundating the audit committee with reports on less important issues, which in turn would detract from the committee's core responsibility of focusing its oversight on the most important audit issues. Accordingly, we recommend the Final Guidelines expressly state that internal audit need only provide the audit committee reports and risk assessments related to material or aggregate risks, and amended audit plans only in the event of a material change, and that there is no expectation that the volume of such reports is supposed to increase significantly as a result of the Guidelines.

C. Inventory of Businesses

The Proposed Guidelines would require internal audit to maintain a complete and current inventory of all of the Bank's material businesses, product lines, services, and functions. The Preamble requests comment on whether IRM should also maintain such an inventory in order to ensure that internal audit has identified all material businesses, product lines, services, and functions.

While we support the principle that the risk management framework needs effective checks and balances, the Final Guidelines should specify that it is sufficient for either internal audit or IRM to maintain the inventory, but that maintaining duplicate (and potentially inconsistent) inventories is not required. Requiring both IRM and internal audit to create separate inventories would require significant, redundant efforts, with little marginal benefit in terms of risk management. Indeed, Banks should have the flexibility to assign maintenance of the inventory to either IRM or internal audit, based on the Bank's particular circumstances and needs. The Final Guidelines should also expressly

---

[40] *Id.* at 5

[41] 79 Fed. Reg. at 4299 (col. 1).

[42] 79 Fed. Reg. at 4298 (col. 1) (emphasis added).

acknowledge that front-line units are expected to play a significant role in the creation of the inventory as well.

Finally, many banking organizations maintain what might be better described as an "audit universe," as opposed to an "audit inventory," which is built around activities and processes that should be subject to audit and which is generally not the equivalent of an inventory of every business, product, service and function. Such an approach is consistent with guidance published by the Federal Reserve, under which internal audit is required to "identify all auditable entities within the audit universe" as part of its audit methodology.[43] In addition, having internal audit create the "audit universe" is consistent with the established principle of an "independent" audit function. The Final Guidelines should clarify that use of such an "audit universe," developed by internal audit, on which to base the audit plan would not be problematic as long it encompasses all material risks.

D. Benchmarking Against Leading Industry Practices

The Proposed Guidelines would require internal audit to conduct an independent assessment annually of the design and governance of the Bank's risk governance framework. This independent assessment would be required to "include a conclusion on . . . the degree to which the bank's risk governance framework is consistent with leading industry practices."[44] The Preamble requests comment on whether such an assessment is 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.

The Clearing House believes that there is merit for boards and management to be informed by risk governance and management practices applied by other firms within the financial services industry; however, Banks often have very different organizational structures, businesses, strategies, risk appetites, and risk governance frameworks that are responsive to different competitive situations and stakeholder expectations. Given these idiosyncratic circumstances, it would be very difficult to discern "leading industry practices," especially since there is no recognized standard-setting body for risk management practices. And even if it were possible to discern "leading industry practices," benchmarking a Bank with unique risk characteristics against those practices would likely be extremely difficult. Moreover, evaluating the consistency of risk governance frameworks with "leading industry practices" does not align with the assurance role and responsibilities of internal audit. In addition, as a practical matter, many Banks may feel the need to engage a third party to assist internal audit in conducting such an evaluation. As a practical matter, such a requirement may lead to greater use of third party consultants offering to provide guidance in this regard; we question whether the potential benefits would outweigh the costs of such an engagement.

For all these reasons, we recommend that the Final Guidelines omit any requirement to benchmark against leading industry practices.

---

[43] Federal Reserve, *Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing*, at 8-9 (January 23, 2013).

[44] 79 Fed. Reg. at 4288, (col. 2).

E. Clarification of Internal Audit Risk-Rating Responsibilities

The Proposed Guidelines specify that internal audit must design and implement an audit plan that "should rate the risk presented by each front line unit, product line, service, and function. . . . 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."[45]

It is not clear whether the "Bank-wide risk assessments" described in this passage are risk assessments that would be prepared by internal audit on a basis independent of management (either front-line units or IRM) or whether the risk assessments would be prepared by, or in conjunction with, front-line units and/or IRM. The Final Guidelines need to clarify this point. We also request clarification regarding the basis on which internal audit "should periodically adjust these ratings based on risk assessments conducted by front line units," while at the same time sustaining the independence and objectivity of the internal audit function.

V. Expected Level of Documentation

The Proposed Guidelines specify certain documentation requirements, *e.g.,* written policies, inventory of material businesses, audit plan, risk appetite statement, and strategic plan. Apart from these specific requirements, the Proposed Guidelines do not discuss the level of documentation expected for Banks to demonstrate compliance with the new requirements. That appears to be intentional, with Banks having flexibility to decide how much documentation is necessary. But we also believe that it would be useful for the Final Guidelines to confirm that they are not intended to impose significant new documentation and reporting burdens, and that often the expectations can be met through informal conversations and communications with examiners.

VI. Other Issues

In addition to the specific requests for clarification noted above, The Clearing House believes the following technical changes should be made in the Final Guidelines to further clarify the OCC's expectations:

- The required risk assessment under the three-year strategic plan should adopt a materiality threshold in determining the risks that must be assessed. The Proposed Guidelines specify that a Bank's CEO must develop the three-year strategic plan with input from the three lines of defense, and the plan must contain a comprehensive assessment of risks that currently impact the Bank *or could impact the Bank* during the period covered by the plan, among other things.[46] On its face, this standard is overly broad. The Final Guidelines should expressly state that the assessment should only apply to *material* risks that currently impact the Bank or could impact the Bank. Also, it should be clarified that the CEO should oversee the plan or be accountable for the plan, but not be responsible for *developing* the plan, and that internal audit's role should be limited, in order to ensure that the independence of the function is not jeopardized.

[45] 79 Fed. Reg. at 4288 (col. 1).

[46] 79 Fed. Reg. at 4299 (col. 1).

- The Proposed Guidelines would require the CEO to oversee the "day-to-day" activities of the CRE and CAE (although in the latter case, that function could be fulfilled by the board's audit committee).[47] The Preamble to the Proposed Guidelines further suggests that this will require oversight of these executives' "administration" of policies and procedures, as well as other detailed and specific tasks. Such requirements seem too prescriptive and management-oriented for a board committee (in the case where the audit committee maintains oversight responsibility over the CAE). But even for a CEO, whose job obviously is to manage, the "day-to-day" and "administration" language suggests a level of involvement that is too prescriptive. While the CEO should be accountable for such activities, he or she should not be required to be personally involved in such day-to-day activities of other executives. Accordingly, we request that this language be modified in the Preamble to the Final Guidelines to recognize that neither a board committee nor the CEO should be expected to become so involved in the details of IRM or internal audit activities.

- Similar to our comment on the use of the term "ensure" with respect to the board of directors, we believe that the Final Guidelines should not use the term "ensure" when discussing concentration and front-line unit risk limits.[48] Rather, the limits should control excessive risk-taking. We would propose that the Guidelines be revised to state as follows: "Concentration and front line unit risk limits should control excessive risk-taking and, when aggregated across such units, should be aligned with the limits established in the Bank's risk appetite statement."

- The Final Guidelines should clarify whether they will replace or supersede all previous correspondence and guidance from the OCC regarding its Heightened Expectations, including previous examiner guidance.

VII. Need for Appropriate Transitional Period

Finally, although Banks have been adjusting their risk management frameworks to comply with the OCC's Heightened Expectations for the last three years, there are aspects of the Guidelines, as described above, that are new. In addition, at the same time that Banks will have to make adjustments to comply with the Final Guidelines, their consolidated holding companies will be making adjustments to their enterprise-wide risk management frameworks to comply with the Federal Reserve's recently finalized regulation establishing Enhanced Prudential Standards.[49] Finally, by issuing these formal Guidelines as part of Part 30, the OCC intends for the consequences of failing to comply with its Heightened Expectations to be more severe: enforcement will be facilitated.

Accordingly, given the changes that will need to be made and the severe consequences that could follow from a failure to comply, The Clearing House believes that the Final Guidelines should include an appropriate transitional period pursuant to which Banks are given at least one year from final publication to achieve full compliance.

---

[47] 79 Fed. Reg. at 4297 (col. 3), 4298 (col. 1).

[48] 79 Fed. Reg. at 4299 (col. 2).

[49] Federal Reserve, *Enhanced Prudential Standards for Bank Holding Companies and Foreign Banking Organizations*, Docket No. 1438 (February 18, 2014).

* * *

The Clearing House appreciates the opportunity to provide comments on the OCC's Proposed Guidelines. Should you have any questions or need further information, please contact Jeremy Newell at 202-649-4662 (email: jeremy.newell@theclearinghouse.org), Jennifer Scott at 212-612-9280 (email: jennifer.scott@theclearinghouse.org) or the undersigned at 212-612-9220 (email: gregg.rozansky@theclearinghouse.org).

Respectfully Submitted,

Gregg L. Rozansky
Managing Director and Senior Associate General Counsel The Clearing House Association L.L.C.

cc: Honorable Thomas J. Curry
Comptroller of the Currency

Martin Pfinsgraff
Senior Deputy Comptroller for Large Bank Supervision

John C. Lyons
Senior Deputy Comptroller Bank Supervision Policy and Chief National Bank Examiner

Amy Friend
Senior Deputy Comptroller and Chief Counsel

Molly Scherf
Deputy Comptroller Large Banks

Stuart Feldstein
Director for Legislative and Regulatory Activities

Andra Shuster
Senior Counsel, Legislative & Regulatory Activities Division

Martin Chavez
Attorney, Securities and Corporate Practices Division

John Dugan
Partner, Covington & Burling LLP

Gregory Frischmann
Associate, Covington & Burling LLP