THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 • www.rmahq.org

December 18, 2013

Via E-Mail

Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Washington, D.C. 20219
John Eckert
Director, Operational Risk and Core Policy

Re: OCC 2013-29, Third-Party Relationships

Dear Mr. Eckert:

This letter is submitted by The Risk Management Association ("RMA" or the "Association") in respect of the OCC's recently issued Risk Management Guidance, "Third Party Relationships," dated October 30, 2013 (the "New Guidance"), which rescinds OCC Bulletin 2001-47, "Third Party Relationships: Risk Management Principles," and OCC Advisory Letter 2000-9, "Third Party Risk" (together, the "Old Guidance").

In the United States, corporate governance traditionally has been carefully balanced between the board of directors, which is charged with policy formulation and oversight, and senior management, which is charged with execution of policy and strategy and the day-to-day operations of the business. In the wake of Sarbanes-Oxley and the Dodd-Frank Act, the traditional system of corporate governance has undertaken a fundamental shift as the regulatory agencies have shifted responsibilities to the board that had formerly been the province of management. We note that the New Guidance reflects this shift of managerial responsibility to the board, which bears further examination. RMA respectfully requests that the OCC revise the New Guidance to be principles-based and harmonize the New Guidance to mirror the guidance issued by the Federal Reserve Board on December 5, 2013.

RMA is concerned that the New Guidance reflects a shift in tone and expectation regarding the role of the board of directors, namely that the board, insofar as third party risk management is concerned, appears to be required to function not as a board, but rather, as simply another layer of management. RMA is concerned that this is a slippery slope and that boards will increasingly be required to function like management. Requiring boards to become engaged in an increasing amount of day-to-day activities that are properly in the domain and expertise of management has the unintended consequence of diluting the effectiveness of board governance. It will become increasingly difficult for boards to provide effective oversight if boards are engaged as a decision-maker or are involved in the operations of the bank.

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 • www.rmahq.org

Introduction

RMA is a 501(c)(6) not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk principles in the financial services industry. RMA helps its members use sound risk principles to improve institutional performance and financial stability and enhance the risk competency of individuals through information, education, peer-sharing and networking. RMA has 2,600 institutional members that include banks of all sizes as well as nonbank financial institutions. They are represented in the Association by more than 16,000 risk management professionals who are chapter members in financial centers throughout North America, Europe, and Asia/Pacific.

One of the most important components of RMA's mission is to provide independent analysis on matters pertaining to risk and capital regulation. In this regard, the comments contained herein are informed by subject matter experts from member institutions of the Association, including RMA's Vendor Management Roundtable.

While the OCC has not requested comment on the New Guidance, RMA is submitting this letter to note its concern that boards of directors of banks ("bank boards") are (i) facing increasing documentation burdens and (ii) increasing their scope or mandate beyond their advisory and oversight functions into actual management of the bank.

RMA notes that the American Association of Board Directors has identified over 800 legislative and regulatory provisions that have accumulated over many decades that impact the responsibilities of bank directors. We submit that the ever-increasing regulatory burden creates a significant distraction from board time necessary for effective risk oversight and other essential board responsibilities. The increasing threat of regulatory and personal liability is forcing bank boards to become "compliance" boards where attention must be focused on satisfying laws, regulations, and regulatory guidance that pertain to duties that are properly the function of day-to-day management.

The New Guidance provides an opportunity for RMA to share these concerns with the OCC in the hopes of creating a dialogue between the regulatory community and the industry to improve corporate governance from a risk management perspective. RMA is not providing commentary with respect to the New Guidance *in toto*, but instead is confining its comments at the present time to the role of the Board of Directors in approving contracts with third parties in respect of critical activities undertaken by a bank.

The Proper Role of Bank Boards

Bank boards play a critical role in promoting safety and soundness. This is increasingly clear, particularly in the wake of the financial crisis and the passage of the Dodd-Frank Act. Bank

boards have a dual mandate, comprised of an advisory capacity and an oversight function. When acting in an advisory capacity, bank boards should consult with management regarding the strategic and operational direction of the bank, which is informed by and measured against the bank's risk appetite policy.

We respectfully submit that the regulatory community and industry alike have recognized that a well-functioning financial system requires that banks take prudent risk positions that generate an appropriate level of earnings. Accordingly, a bank's risk level should be informed by its risk appetite, which is adopted by the bank board. As the industry continues to recover from the financial crisis, banks increasingly are focusing on aligning their risk taking activities with their stated risk appetite.

In discharging its risk oversight function, bank boards should monitor bank performance against risk appetite and other metrics. Bank boards should be receiving high level information and key risks of concern in the context of informative and actionable reports from management. However, it is management that is responsible for the bank's risk management not the board, which is merely charged with risk oversight.

We respectfully submit that effective bank boards satisfy both functions described above. Importantly, we would also note that the responsibilities of the bank board are separate and distinct from those of management. The bank board does not, and should not, manage the bank.

Commentary Regarding the New Guidance

As a precatory matter, RMA believes that the Old Guidance was well accepted by the industry, and that while industry participants are (were) in different stages of maturity with respect to their vendor management programs under the Old Guidance, the Old Guidance appeared to have its intended effect, namely, that bank boards and management properly oversee and manage third-party relationships, respectively. RMA notes that the Old Guidance could fairly be described as principles based such that banks were able to design vendor management programs commensurate with their size, scale and complexity. In comparison, the New Guidance is much more prescriptive and RMA has serious concerns about the unintended consequences of the New Guidance on corporate governance, particularly with respect to bank boards. While there appear to be some signs of convergence on certain aspects of vendor management programs, RMA believes that there should not be an expectation that all aspects of practice will eventually converge, and hence the supervisory community should continue to apply a principles□based approach, as opposed to a prescriptive one, to the development and implementation of vendor risk management programs. In short, the New Guidance raises three broad areas of concern, each of which is more fully described below.

The role of bank boards cannot be underestimated. While conceptually, RMA does not disagree with the fundamental objective set forth in the New Guidance, namely, that the use of third parties to perform "critical activities" for and on behalf of a bank requires the establishment of risk management processes commensurate with the level of risk and complexity of the bank's

third party relationships, RMA is growing increasingly concerned that the mandate of bank boards has been expanded such that bank boards are now becoming involved in issues traditionally reserved to senior management, and being required to confirm decisions made by senior management in the ordinary course of business.

1. **The definition of the term "critical activities" is overly broad and will place an unreasonable burden on bank boards in the context of reviewing arrangements for critical activities, diluting bank boards' advisory and other risk oversight responsibilities.**

The New Guidance requires bank boards to (i) review and approve management plans for using third parties that involve critical activities; (ii) review summaries of due diligence results and management's recommendations to use third parties that involve critical activities, and (iii) review and approve contracts with third parties; (iv) review the results of management's ongoing monitoring of third-party relationships involving critical activities; (v) ensure that management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring; and (vi) review results of periodic independent reviews of the bank's third-party risk management process.

RMA has two fundamental concerns in this regard: (i) that bank boards will be confronted with a larger than intended volume of third party-critical activity management, plans, due diligence reports and contracts to review and approve, and (ii) that in order to discharge their fiduciary duties in reviewing and approving such plans, due diligence and contracts, bank boards will be required to take an increasingly granular (i.e., managerial) approach to the review and approval of such items, which as a consequence means that bank boards will have less time available to engage in their advisory and risk oversight capacities.

As to the first issue, the definition of the term "critical activities" is overly broad and may have the unintended consequence of causing boards to take an increasingly granular look at third party operations, which is squarely within the purview of senior management. The New Guidance defines the term "critical activities" as meaning "significant bank functions" and "significant shared services" which *could* (emphasis added) include payments, clearing, settlements, custody and information technology, or other activities that:

(a) *could* cause a bank to face significant risks if the third party fails to meet expectations;

(b) *could* have significant customer impacts;

(c) require significant investment in resources to implement the third-party relationship and manage the risk; or

(d) *could* have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

The above definition is vague and overly broad. The choice of the term "critical activities" implies a heightened state of risk or uncertainty while the use of the term "significant" (in respect of bank functions and shared services) implies a lower standard; i.e., meaning likely to have an effect. *See Merriam Webster's Collegiate Dictionary,* Tenth Edition.

RMA believes that the definition of "critical activities" may become a catch-all, such that almost any activity in which a bank contracts with a third party could arguably fall within the definition and, therefore, the purview of review and approval by bank boards.

Consequently, RMA respectfully suggests that the OCC permit banks to adopt a "materiality" standard in defining "critical activities" that would rise to the level of requiring bank boards to approve the contracts in respect thereof. This should be determined by the bank taking into account its risk appetite and the risk attributes of the third party relationship. By way of example only, a bank may determine that material contracts satisfying the "critical activity" definition might have the following attributes:

(a) Annual expenditures in excess of a material threshold as determined by the relevant bank based upon its size, scale and complexity;

(b) Be determined by management to be an activity that is highly critical to the business from the standpoint of strategic risk and reputational risk;

(c) Require a recovery time of short duration; for example, XX hours or less;

(d) Be an activity by its nature, which would require an extended period of time to either replace the vendor or migrate the service in-house; for example, YY days or more;

(e) Be an activity that is performed off-shore.

Again, the foregoing is simply an example of how an individual bank may approach determining whether particular third party activities rise to the level of "critical activities' under the New Guidance. There may be other factors that a bank would want to consider in making its own determination of whether a particular activity rises to the level of a critical activity triggering the application of the New Guidance. RMA notes that the factors set forth in the example above are all important factors for a bank to consider, but RMA respectfully suggests that the factors used to determine whether an activity is a critical activity should be left up to the reasonable discretion of the individual bank. Similarly, banks should be free to assess the relative importance or weighting of each of the factors that the bank uses in determining whether a particular activity is a critical activity; moreover, we would note that it is not any one single factor or particular prescribed combination of factors that should determine whether a particular activity is a critical activity; rather, depending upon the nature of the activity, different combinations of factors may be appropriate in determining whether an activity is a critical activity. Simply put, expenditures, criticality, reputation risk, recovery time, off-shoring and duration to transition are all important

factors to consider, but it is the ultimate combination of factors that drives risk, not any single element or particular combination of elements.

RMA believes that allowing banks to add a materiality standard with respect to critical activities will help to reduce the burden on bank boards to review third party arrangements. Reducing this burden is important both because bank boards are being required under the New Guidance to function in a managerial capacity and also because, in order to discharge their fiduciary duties as directors in approving third party plans, due diligence and contracts, bank boards will not only need to be cognizant of the business terms of the transaction and the risks associated with such third party, but will also need to have a clear and present understanding of the legal terms of the contract, as well as the other third parties who could have offered the services, the terms that were offered by or could have been offered by such other third parties, and the risks associated with partnering with such other third parties.

As presently written, the New Guidance suggests a material increase in the number of third party arrangements discussed at the bank board level, while also requiring the bank board to approve such plans, due diligence and contracts. Over time, it is likely that directors will get bogged down in minutia better left to management and legal counsel, which frustrates the purpose of the bank board – to advise and provide risk management oversight. As a consequence of placing this risk management burden on bank boards, banks of all sizes – but particularly midsize and community banks – may have a more difficult time attracting and retaining qualified directors given that the burdens of service may not be commensurate with the remuneration offered.

2. Bank boards should be responsible for approving risk-based policies and management should be responsible for developing/approving risk processes and procedures (collectively, "risk processes").

The New Guidance also requires bank boards to, among other things, (i) ensure an effective *process* is in place to manage risks related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite; and (ii) approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities.

RMA believes that the industry would be better served if the New Guidance were revised to be principles-based and mirror the recently issued guidance by the Board of Governors of the Federal Reserve System. RMA believes that the duty to ensure that an effective process is in place to manage risks related to third party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite is better left to the appropriate management group that is responsible and accountable for their execution. RMA further believes that the approval of plans, due diligence and the definitive written agreement dealing with vendor contracts is also a matter reserved for management and not the bank board, absent any specific agreement for a critical activity meeting or exceeding a bank's internal materiality standard as described hereinabove.

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 • www.rmahq.org

Conclusion

In conclusion, RMA is very concerned that bank boards are increasingly focused on details concerning the daily activities of banks. The overburdening of bank directors with responsibilities that are insignificant or that are better delegated to management is a serious public policy issue. Bank directors need to focus on the important issues facing their banks to meet their fundamental duties of care and loyalty. They are not full-time bank officers or employees and in most cases, they are not professional bankers.

The involvement of bank boards at the granular level set forth in the New Guidance involves the practice of risk management, as opposed to risk oversight, which will have the unintended consequence of diluting the time and attention that bank boards can give to other matters that are squarely within their advisory and risk management purview.

There is virtually no recognition in the federal banking laws, regulation and guidance that it is prudent and consistent with a board's fiduciary duties for the board to rely reasonably on management and advisors. Yet this is the foundation of modern American corporate law. Every state recognizes either in statute or case law that corporate board members may reasonably rely on their management or on their opinions, information, reports and statements.

RMA believes that bank boards should provide strategic direction and vision through the establishment of broad goals and objectives. Similarly, RMA continues to believe that the senior management should be charged with conducting the day-to-day activities of the bank and taking the necessary actions to achieve the goals and objectives established by the board, which may include contracting with third parties. The corporate governance framework should ensure the strategic guidance of the bank, the effective monitoring of management by the board, and the board's accountability to the bank and the shareholders.

* * * * *

Should there be any questions concerning the comments reflected above, kindly contact Edward J. DeMarco, Jr., General Counsel and Director of Regulatory Relations at (215) 446-4052 or edemarco@rmahq.org.

Very truly yours,

Edward J. DeMarco, Jr.,
General Counsel and
Director of Regulatory Relations

cc: John C. Lyons, Jr.