ISSUE 4

OCC Clarifies Its Expectations in Updated Guidance for Handling Third-Party Relationships

In October 2013, the Office of the Comptroller of the Currency (OCC), the U.S. regulator of national banks, issued Bulletin 2013-29—guidance for assessing and managing risks associated with third-party relationships. The OCC defines a third-party relationship as "any business arrangement between a bank and another entity, by contract or otherwise."[1] This bulletin rescinded earlier guidance and supplemented other OCC and interagency issuances on third-party relationships and risk management. OCC makes clear at the beginning that the guidance applies to all banks with third-party relationships, including community banks.

In the guidance, the OCC provides considerable detail on the risk management life cycle and concludes with a section on supervisory reviews of third-party relationships. It contains two appendices—risks associated with third-party relationships and references.

BACKGROUND

The OCC notes that banks continue to increase the number and complexity of relationships with both foreign and domestic third parties and expresses concern that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships. Examples of these relationships include outsourcing, relying on a single third party to perform multiple activities, working with third parties that engage directly with customers, contracting with third parties that subcontract activities, and working with third parties to address deficiencies in bank operations or compliance with laws or regulations. The OCC identifies deficiencies in banks' risk management processes that include bank management failure to properly assess and understand the risks and direct and indirect costs involved in third-party relationships, failure to perform adequate due diligence and ongoing monitoring, failure to assess a service provider's risk management practices before entering into a contract, entering contracts that

[1] Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records.

incentivize the service provider to take risks that increase revenue but that may be detrimental to the bank and its customers, and engaging in informal relationships without contracts.

RISK MANAGEMENT PROCESSES

The OCC expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures. Therefore, the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve what the OCC deems to be "critical activities"—significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology) or other activities that

- could cause a bank to face significant risk if the third party fails to meet expectations,
- could have significant customer impacts,
- require significant investment in resources to implement the third-party relationship and manage the risk, and/or
- 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.

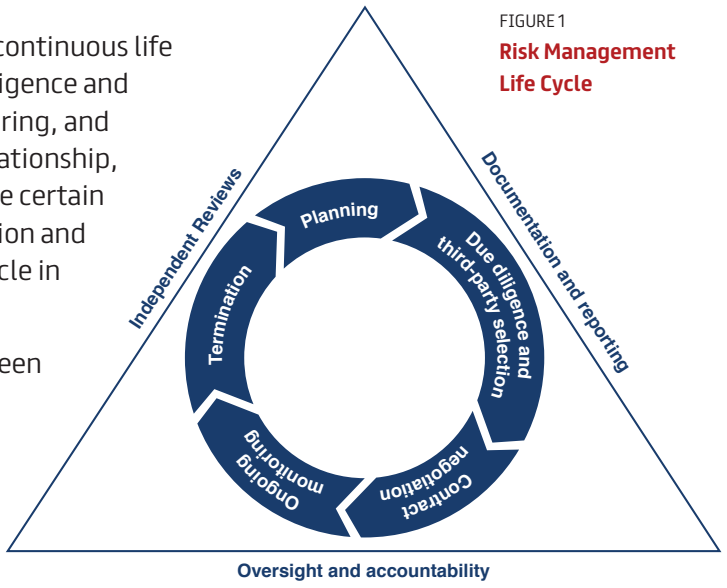
The OCC makes it clear that failure to have an effective third-party risk management process may be *an unsafe and unsound banking practice.*

RISK MANAGEMENT LIFE CYCLE

An effective third-party risk management process follows a continuous life cycle for all relationships and incorporates planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination. In addition, throughout the life cycle of the relationship, as part of its risk management process, bank employees have certain responsibilities—oversight and accountability, documentation and reporting, and independent reviews. The OCC depicts this cycle in Figure 1.

In each area, the Bulletin differentiates to some extent between specific references that are expressed as a mandate through the use of strong affirmative language and other somewhat softer "best practices" that are identified through reference to actions a bank should "consider" taking.

FIGURE 1
Risk Management Life Cycle



Source: OCC

PLANNING

Before entering into a third-party relationship, a bank's senior management should develop a management plan for its third-party relationships. This plan should account for, among other things, risks associated with the activity, the strategic purposes, the legal and compliance aspects, the complexity of the relationship, the cost to control the risks, the nature and handling of customer interactions, implications for information security, specific laws and regulations applicable to the third-party activity, how the bank will monitor

and assess compliance, and whether the relationship is consistent with the bank's broader corporate policies. The plan should be presented to and approved by the bank's board of directors when critical activities are involved.

DUE DILIGENCE AND THIRD-PARTY SELECTION

With regard to the conduct of due diligence on potential third parties, a bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations in a safe and sound manner. More extensive due diligence is needed when a third-party relationship involves critical activities. Further, on site visits may be useful to understand the third party's operations and capacity. Senior management should review the results of the due diligence review to determine whether the third party is able to meet the bank's expectations and whether the bank should proceed with the relationship. For third-party relationships that involve critical activities, management should present the results to the board.

During due diligence, banks should consider the third party's:

- **Overall business strategy and goals** to ensure they do not conflict with those of the bank.
- **Legal and regulatory compliance** program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with domestic and international laws and regulations.
- **Financial condition**, including reviews of its audited financial statements.
- **Business experience and reputation**, including its depth of resources and previous experience providing the specific activity.
- **Fee structure and incentives** for similar business arrangements to determine if they would create burdensome upfront fees or result in inappropriate risk taking by the third party or the bank.
- **Qualifications, backgrounds, and reputations of company principals** (ensure the third party conducts thorough background checks).
- **Risk management program**, including policies, processes and internal controls.
- **Information security program**—does the third party have sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities?
- **Business processes and technology** that will be used to support the activity.
- **Ability to respond to service disruptions or degradations** resulting from natural disasters, human error, or intentional physical or cyber attacks.
- **Physical and environmental controls** to ensure safety and security of facilities, technology systems, and employees.
- **Human resource management** including training and succession planning.

- **Reliance on subcontractors** including the volume and types of subcontracted activities and the subcontractors' locations.
- **Insurance coverage** to insure against losses attributable to dishonest or negligent acts, and hazards such as fire, loss of data, and protection of documents.
- **Conflicting contractual arrangements with other parties** as such arrangements may transfer risks to the bank.

CONTRACT NEGOTIATION

Once a third party has been selected, bank management should negotiate a contract that clearly specifies the rights and responsibilities of each party to the contract. Senior management should obtain board approval before contract execution when a third-party relationship will involve critical activities. Contracts should be reviewed periodically, particularly those that involve critical activities, to ensure they continue to address pertinent risk controls and legal protections. Areas to be addressed in contracts include: the nature and scope of the arrangement; performance measures or benchmarks; responsibilities for providing, receiving, and retaining information; the right to audit and require remediation; responsibility for compliance with applicable laws and regulations; cost and compensation; ownership and license; confidentiality and integrity; business resumption and contingency plans; indemnification; insurance; dispute resolution; limits on liability; default and termination; customer complaints; subcontracting; foreign-based third parties; and OCC supervision.

ONGOING MONITORING

Ongoing monitoring is an essential component of the bank's risk management process and more comprehensive monitoring is necessary when third-party relationships involve critical activities. Banks should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party commensurate with the level of risk and complexity of the relationship. The bank's ongoing monitoring should cover the due diligence activities discussed earlier and ensure that ongoing monitoring adapts as the level and types of risk change over the course of the relationship. Bank controls to manage risks from third-party relationships should be tested regularly, particularly where critical activities are involved. Management should respond to issues when identified including escalating significant issues to the board.

TERMINATION

Management should ensure that relationships terminate in an efficient manner and have a contingency plan to bring the service in-house if there is no alternative third party. The extent and flexibility of termination rights may vary with the type of activity.

BANK STAFF RESPONSIBILITIES

The Bulletin also recommends that a bank's board of directors, senior management, and bank employees that directly manage third-party

relationships focus on three key areas throughout the relationship—oversight and accountability, documentation and reporting, and independent reviews.

OVERSIGHT AND ACCOUNTABILITY

The bank's board of directors (or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes. The OCC details distinct but interrelated responsibilities for the board, senior management, and employees within the lines of business who manage the third-party relationships. These responsibilities are to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities.

- **Board:** ensure effective risk management processes are in place, approve risk-based policies that govern the third-party risk management process and identify critical activities, review and approve management plans and contracts for using third parties that involve critical activities, review summary reports of due diligence and on-going monitoring of relationships involving critical activities, ensure management takes appropriate action to remedy significant deterioration in performance, review results of periodic independent reviews.
- **Senior management:** develop and implement the bank's third-party risk management policies and processes; identify those that involve critical activities and present plans to the board when such activities are involved; ensure appropriate due diligence and present results to the board when making recommendations to use third parties that involve critical activities; review and approve contracts and seek board approval for those that involve critical activities; ensure ongoing monitoring, documentation, and reporting of third-party relationships; ensure periodic independent reviews of relationships that involve critical activities; hold accountable employees managing third-party relationships; terminate agreements that no longer align with the bank's strategies or where the vendor is not meeting expectations; and oversee enterprise-wide risk management and reporting of third-party relationships.
- **Employees:** conduct due diligence and ongoing monitoring of third parties, ensure compliance, address or escalate issues, keep third parties informed of bank operational issues, ensure regular testing of controls to manage risks, maintain appropriate documentation, respond to material weaknesses, and recommend termination where appropriate.

DOCUMENTATION AND REPORTING

Banks should properly document and report on their third-party risk management process and specific arrangements throughout their life cycle. Proper documentation includes: a current inventory of all third-party relationships, approved plans for the use of third-parties, due diligence results, cost analysis, executed contracts, regular risk management and performance reports received from the third party, regular reports to the board and senior management on results of internal control testing and ongoing monitoring of third parties involved in critical activities, and regular reports to the board and

senior management on the results of independent reviews of all of the banks' overall risk management process.

INDEPENDENT REVIEWS

Senior management is responsible for ensuring that periodic independent reviews are conducted on the third-party risk management process, particularly when a bank involves third parties in critical activities. These reviews can be done by the bank's internal auditor or an independent third party. Senior management is responsible for ensuring the results are reported to the board. Senior management should analyze the results of these reviews, make appropriate adjustments to the risk management process, respond promptly and thoroughly to significant issues or concerns, and escalate to the board if the risk posed is approaching the limits of the bank's risk appetite.

SUPERVISORY REVIEWS OF THIRD-PARTY RELATIONSHIPS

The OCC expects bank management to engage in the analytical process necessary to identify, measure, monitor, and control the risks associated with third-party relationships and to avoid excessive risk taking that may threaten a bank's safety and soundness. In this section, the Bulletin outlines expectations for examiners when reviewing third-party relationships to determine the degree to which the bank has an effective risk management process that is commensurate with the level of risk, complexity of third party relationships, and organizational structure of the bank.

When reviewing third-party relationships, examiners should: assess the bank's ability to oversee and manage relationships; highlight and discuss material risks and any deficiencies with the board and senior management; and review the bank's plans for remediation of deficiencies, particularly those deficiencies that involve critical activities. When circumstances warrant, the OCC may use its authority to examine the functions or operations performed by a third party on the banks' behalf.[2] The OCC is clear that it will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the bank or its third party. In addition, the OCC may assess a bank a special examination or investigation fee when it examines or investigates a third party for the bank.

RISKS ASSOCIATED WITH THIRD-PARTY RELATIONSHIPS

The OCC provides a great deal of detail on the risks associated with third-party relationships in an appendix. Use of third parties reduces management's direct control of activities and may introduce new or increase existing risks, specifically, operational, compliance, reputation, strategic, and credit risks and the interrelationship of these risks. Increased risk most often arises from greater complexity, ineffective risk management by the bank, and inferior performance by the third party.

- **Operational risk** is present in all products, services, functions, delivery channels, and processes. Third-party relationships may increase a bank's

[2] Before conducting an examination of a third party that is a functionally regulated affiliate (FRA), the OCC is required to give notice to and consult with the FRA's primary regulator and, to the fullest extent possible, avoid duplication of examination activities, reporting requirements, and requests for information.

exposure to operational risk because the bank may not have direct control of the activity performed by the third party.

- **Compliance risk** exists when products, services, or systems associated with third-party relationships are not properly reviewed for compliance or when the third party's operations are not consistent with laws, regulations, ethical standards, or the bank's policies and procedures.
- Third-party relationships that do not meet the expectations of the bank's customers expose the bank to **reputation risk**.
- A bank is exposed to **strategic risk** if it uses third parties to conduct banking functions or offer products and services that are not compatible with the bank's strategic goals, cannot be effectively monitored and managed by the bank, or do not provide an adequate return on investment.
- **Credit risk** may arise when management has exercised ineffective due diligence and oversight of third parties that market or originate certain types of loans on the bank's behalf, resulting in low-quality receivables and loans. Credit risk also may arise from country or sovereign exposure.

Author: Barbara I. Keller, CAMS, CFCS, is currently an independent consultant. For the last four years of her federal career, she was FinCEN's deputy associate director for compliance and enforcement.

About Alacra

Alacra develops workflow applications that enable 300,000 end users at financial institutions, professional services firms and corporations to search for, extract and analyze mission-critical business information.

Alacra has under license the largest collection of premium business information in the world and continuously collects the latest business data and financial events. Alacra aggregates and filters this content. Configurable solutions keep Alacra's clients up-to-date on their customers, prospects, investments, competition, partners and suppliers, driving business development and streamlining operations.

Alacra's mission is to aggregate, integrate, package and deliver business and financial content in ways that are most useful to our clients, which include nine of the top 10 global investment banks, all four major accounting firms, and nine of the top 10 consulting firms.

Contact Us

AMERICAS (HQ)
100 Broadway, Suite 1101
New York, New York 10005
United States
T +1 (212) 363-9620
F +1 (212) 363-9630
E info@alacra.com

EMEA & APAC
125 Old Broad Street, 6th Floor
London EC2N 1AR
United Kingdom
T +44 (0) 20 3059 5765
F +44 (0) 20 3192 5577