OCC Updates Guidance on Third-Party Risk Management

November 12, 2013

On October 30, 2013, the Office of the Comptroller of the Currency (the "OCC") issued updated guidance to national banks and federal savings associations on assessing and managing risks associated with third-party relationships, which include all business arrangements between a bank and another entity (by contract or otherwise).[1] The new guidance introduces a "life cycle" approach to third-party risk management, requiring comprehensive oversight throughout each phase of a bank's business arrangement with consultants, joint ventures, affiliates, subsidiaries, payment processors, computer network and security providers, and other third parties. Rather than mandating a uniform set of rules, however, the guidance instructs banks to adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships. Accordingly, the OCC expects especially rigorous oversight of third-party relationships that involve certain "critical activities."

The revamped guidance reflects the OCC's concern that the increasing risk and complexity of third-party relationships is outpacing the quality of banks' risk management over these outsourcing arrangements. The guidance cautions that a bank's failure to implement appropriate third-party risk management processes may constitute an unsafe and unsound banking practice, and could prompt formal enforcement actions or a downgrade in a bank's CAMELS management rating to less than satisfactory. The severity of these consequences suggests that third-party risk management practices are becoming an increasingly important focus of OCC supervisory efforts.

A. RISK MANAGEMENT LIFE CYCLE

In establishing standards by which banks' third-party risk management will be assessed, the new guidance emphasizes that banks must maintain adequate risk management processes throughout each phase of a third party relationship's life cycle: planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination. Highlights of the prescribed best practices in each life cycle phase are summarized below.

1. Planning

Prior to entering an outsourcing arrangement, a bank's senior management should develop a plan to manage the third-party relationship. This plan should assess the risks and complexity of the outsourced activity, include a cost-benefit analysis of the outsourcing arrangement, and consider the effect that the third-party relationship may have on the bank's customers,

---

[1] See OCC Bulletin 2013-29, *available at* http://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html. The new guidance rescinds OCC Bulletin 2001-47 and OCC Advisory Letter 2000-9.

employees, and strategic initiatives. While prior guidance under Bulletin 2001-47 similarly encouraged banks to develop a risk management plan prior to contracting with third parties, the new guidance adds the following specific recommendations for such risk management plans:

- *Legal and Regulatory Compliance*—The bank's risk management plan should consider whether the outsourced activities are subject to specific laws and regulations (including those relating to privacy and information security, Bank Secrecy Act and other anti-money laundering laws ("BSA/AML"), and fiduciary requirements), and should address plans to ensure compliance with such laws.
- *Information Security*—The bank's risk management plan should assess potential information security implications of contracting with the third party, including the third party's ability to access the bank's systems and confidential information.
- *Contingency Plans*—The bank's risk management plan should include contingency plans for transitioning the outsourced activity to another third party or to an in-house function.

2. Due Diligence and Third-Party Selection

In selecting a third-party service provider, a bank should not rely solely on its experience with a particular third-party provider. Instead, the bank should conduct an objective, in-depth assessment (which assessment should be commensurate with the risk and complexity of the activities) of the provider's ability to perform in a safe and sound manner. The content of the bank's due diligence should focus on areas such as the third party's financial condition, its business experience and reputation in providing the contemplated activity, the qualifications and backgrounds of the third party's principals, and the effectiveness of the third party's risk management program. Although largely consistent with the topics for due diligence prescribed in Bulletin 2001-47, the new guidance adds the following areas that third-party due diligence should focus on:

- *Legal and Regulatory Compliance*—The bank should evaluate the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the internal controls to ensure the bank's compliance with applicable laws and regulations.
- *Information and Physical Security*—The bank should determine whether the third party is sufficiently able to identify and mitigate known and emerging threats to information security, and should thoroughly assess the third party's information technology infrastructure. Similarly, the bank should evaluate the third party's controls to ensure the security of its facilities, technology, and employees.
- *Fee Structure and Incentives*—The bank should evaluate the third party's fee structure to determine whether the fee structure would create burdensome

upfront fees or incentivize either the third party or the bank to take inappropriate risks.

- *Incident Reporting and Management Programs*—The bank should ensure that the third party has clearly documented processes for identifying, reporting, investigating, and escalating incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions. The bank should further ensure that the third party has adequate management programs to provide accountability in the event of any such incidents.
- *Conflicting Contractual Arrangements*—The bank should review the third party's existing contractual arrangements with subcontractors or other parties where the third party has indemnified itself, and should evaluate the legal and financial risks that these contracts pose for the bank.

3. Contract Negotiation

Upon selecting a third-party service provider, the bank's management should negotiate a contract that clearly specifies the rights and responsibilities of the bank and the third party. The guidance lists a number of topics that should be addressed in a bank's third-party service contracts, including compensation for the services to be provided, performance benchmarks, required notifications, licensing, confidentiality, insurance, indemnification and limits on liability, customer complaints, dispute resolution and termination rights. Significantly, the guidance directs banks to ensure the bank's right to audit the third party and relevant subcontractors, and to stipulate that the third party's performance is subject to OCC examination oversight. By contracting with the bank, the third-party service provider would be subject to the OCC's examination and regulatory authority to the same extent as if the third party's operations had been performed by the bank itself.[2] The new guidance expands on the standards for third-party service contracts under prior Bulletin 2001-47 with respect to the following areas:

- *Legal and Regulatory Compliance*—The contract should address compliance with specific laws and regulations applicable to the contemplated activities. The guidance specifically encourages banks to contract for compliance with the privacy and safeguarding of customer information requirements under the Gramm-Leach-Bliley Act, BSA/AML requirements, Office of Foreign Assets Control rules, and applicable consumer protection laws. Contracts should stipulate the frequency of reporting by the third-party service provider and specifically require the provider to maintain policies and procedures that address the bank's right to conduct periodic reviews.

[2] Pursuant to 12 U.S.C. § 1867(c) and 12 U.S.C. § 1464(d)(7)(D), activities outsourced to a third party by a national bank or thrift are subject to regulation and examination to the same extent as if such services were being performed by the institution itself on its own premises.

- *Subcontracting*—The contract should stipulate when and how the third party must notify the bank of its intent to use a subcontractor, and should specify limits to the third party's ability to subcontract the services. For example, the bank should consider limiting the services that can be subcontracted or prohibiting the third party from subcontracting services to certain subcontractors or locations.
- *Business Resumption and Contingency Plans*—The contract should include provisions for transferring the bank's accounts or activities to another service provider "without penalty" in the event of the initial servicer's bankruptcy, business failure, or business disruption.

4. Ongoing Monitoring

While the third-party service contract is in place, the bank should dedicate sufficient staff with the necessary expertise, authority and accountability to oversee the third party's performance. In general, ongoing monitoring efforts should cover the same areas investigated during the due diligence phase, including the third party's financial condition, key personnel, and risk management systems and internal controls. While the prior Bulletin 2001-47 included a similar list of ongoing monitoring best practices, the new guidance adds the following areas on which banks should focus throughout the third party's performance:

- *Legal and Regulatory Compliance*—The bank should monitor the third party for compliance with all applicable laws and regulations.
- *Information Security*—The bank should monitor the third party's information technology, its processes for responding to emerging threats to information security, and its ability to maintain the confidentiality and integrity of the bank's information and systems.
- *Subcontracting*—The bank should monitor the third party's reliance on, exposure to, or performance of subcontractors, and the extent to which the third party's agreements with other entities may pose a conflict of interest or other risk to the bank.

5. Termination

Unlike the prior Bulletin 2001-47, the new guidance includes a termination phase in the life cycle of a bank's third-party relationships, and requires a bank's risk management controls to continue through this termination phase. Bank management should ensure that third-party relationships terminate in an efficient manner, and should develop a contingency plan to be used in the event of the third party's default or termination of the contract. This contingency plan should address data retention and destruction, the handling of joint intellectual property, mitigation of reputational risks, and continued compliance with applicable laws and regulations.

B. THIRD-PARTY RELATIONSHIPS INVOLVING "CRITICAL ACTIVITIES"

While the OCC will scrutinize all outsourcing arrangements between banks and third-party providers, the guidance indicates that third-party relationships involving certain "critical activities" will be subject to heightened risk management standards. These "critical activities" include significant bank functions (such as payments, clearing, settlements, and custody), significant shared services (such as information technology), and other activities that could significantly impact customers, require significant investment in resources to implement the relationship and manage the risk, impose significant risk to the bank if the third-party fails to meet expectations, or have a major impact on bank operations if the bank has to find an alternate vendor or service provider or if the outsourced activity has to be brought in-house.

The new guidance advises more rigorous attention at all phases of the relationship life cycle, from planning through due diligence and monitoring, for arrangements involving critical activities. The guidance specifically requires board approval of such arrangements, as well as greater senior management and board involvement in the negotiation and monitoring of such arrangements.

C. RESPONSIBILITIES OF BANK EMPLOYEES

In addition to the best practices recommendations specific to each phase of the third-party relationship's life cycle, the new guidance applies the following risk management standards continuously throughout all phases of the third-party relationship's life cycle:

- *Oversight and Accountability*—Clearly delineated roles for the board, management, and employees who manage third-party relationships are outlined to ensure that the outsourced activities are managed effectively.
- *Documentation and Reporting*—A bank should properly document and report its current inventory of all third-party relationships and contracts, with clear identification of those involving critical activities and the risks they pose on an enterprise-wide basis; due diligence results for pending third-party relationships; and regular reports on third-party risk management.[3]
- *Independent Reviews*—A bank should ensure that periodic independent reviews are conducted on its third-party risk management process, particularly those involving critical activities. These independent reviews may be conducted by the bank's internal auditor or by an independent third party. Senior management should analyze the results of such reviews to determine whether and how to adjust the bank's third party relationship and

[3] Banks should ensure that their inventories of third-party relationships and contracts are indeed current. This is particularly important because examiners will expect a current inventory to be made available upon request, and the guidance suggests that the statutory notification requirement under 12 U.S.C. § 1867(c) and 12 U.S.C. § 1464(d)(7)(D), as applicable (which requires national banks and thrifts to notify the OCC within 30 days of making a service contract with a third party or the performance of the service, whichever occurs first), would be satisfied by such an inventory.

the related risk management process, and should escalate significant issues to the bank's board of directors.

D. OBSERVATIONS

In light of the OCC's new guidance, banks should review their third-party risk management policies and processes to ensure that the bank is able to exercise sufficient oversight in each stage of the third-party relationship's life cycle. The guidance suggests that banks should be especially aware of the possible need to update third-party risk management policies related to legal and regulatory compliance, information security, and subcontractors. A bank should likewise consider reassessing its third-party risk management policies if the bank outsources critical activities or entire bank functions to third parties, relies on a single third party to perform multiple activities, or contracts with third parties to engage directly with customers, as the OCC views these third-party relationships as presenting a heightened level of risk and complexity for the bank.

Below are some additional observations:

- *An Interagency Focus on Third-Party Relationships*—The OCC's new guidance joins other recent regulatory pronouncements on the need to effectively monitor and assess the activities of outside vendors. Recently, the Federal Deposit Insurance Corporation issued two supervisory guidance letters on payment processing relationships,[4] and the Consumer Financial Protection Bureau issued guidance on its expectations for the banks and nonbanks it supervises to manage the risks of service provider relationships.[5] And just today, the OCC released separate guidance on the use and review of independent consultants required to be employed by banks and federal branches or agencies in connection with enforcement actions.[6] In general, banks should expect third-party risk management practices to become an increasingly important focus of examination and enforcement.
- *An Emphasis on "Independent" Reviews*—The new guidance references independent reviews or audits of a bank's risk management process or of a third-party provider's internal controls more than a dozen times.
- *Board Attention Is Key*—A significant aspect of the guidance is the requirement that a bank's board of directors approve contracts with, and review the ongoing monitoring of, third parties that involve critical activities. It is clear that the OCC expects a bank's board to be very attentive on an ongoing basis to contractual arrangements involving critical activities, as the

---

4 *See* FDIC Financial Institution Letters 3-2012 and 43-2013.

5 *See* CFPB Bulletin 2012-03.

6 *See* OCC Bulletin 2013-33. Among other things, the guidance details the OCC's expectations for assessing the independence of a consultant used by a bank in connection with an enforcement action, as well as the required terms for any proposed engagement contract and work plan.

guidance emphasizes the board's review of due diligence results, management's recommendations, and periodic independent testing of the bank's third-party risk management process.

- *Diligence on a "Vendor's Vendors"*—Banks will need to be particularly mindful of issues relating to a third party's vendors. In particular, due diligence efforts should focus on, among other things, the information technology systems and data security providers relied upon by banks' loan review consultants, outside counsel, payment processers, website hosting providers, and others.

* * *

For more information, please contact a member of Simpson Thacher's Financial Institutions Group.

Lee Meyerson
(212) 455-3675
lmeyerson@stblaw.com

Maripat Alpuche
(212) 455-3971
malpuche@stblaw.com

Elizabeth Cooper
(212) 455-3407
ecooper@stblaw.com

Mark Chorazak
(212) 455-7613
mchorazak@stblaw.com

Spencer Sloan
(212) 455-7821
spencer.sloan@stblaw.com

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
2 Houston Center
909 Fannin Street
Houston, TX 77010
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000