Risk Management of Third Party Relationships: – OCC Guidance

Executive Summary

The Office of the Comptroller of the Currency (OCC) released Bulletin 2013-29 on October 30, 2013, to provide updated guidance to national banks and Federal savings associations (collectively, Banks) on effective risk management of third-party relationships. The OCC states that it is concerned "the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships" adding that "a bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws."

OCC Bulletin 2013-29 is applicable to all Banks with third-party relationships, defined as "any business arrangement between a bank and another entity, by contract or otherwise." The OCC expects risk management processes to be scaled to the level of risk and complexity in a Bank's third-party relationships and provide for more comprehensive and rigorous oversight of third-party relationships that involve "critical activities." The OCC indicates that failure to have an effective third-party risk management process commensurate with the level of risk, complexity of third-party relationships, and the Bank's organizational structure may be considered an unsafe and unsound banking practice.

To be effective, the OCC states that the third-party risk management process should follow a continuous life cycle for all relationships, including the following phases:

- Planning (incorporating risk strategy, identification of inherent risks of activities, and use of third-parties)
- Due diligence and third-party selection
- Contract negotiation
- Ongoing monitoring
- Termination, including contingency plans
- Roles and responsibilities for oversight and relationship management
- Documentation and reporting
- Independent review.

Of specific note, the OCC has called for Banks to conduct periodic independent reviews on the third-party risk management process, particularly when third parties are involved in critical activities. The Bank's internal auditor or an independent third party may perform the reviews, and senior management should ensure the results are reported to the board.

Background

OCC Bulletin 2013-39 rescinds OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," and OCC Advisory Letter 2000-9, "Third-Party Risk."

The OCC notes that Banks continue to increase the number and complexity of relationships with both foreign and domestic third parties. It has observed certain industry trends that, given the increasing number and complexity of these relationships, reinforce the need for effective risk management. These observations include "instances in which Bank management has:

- Failed to properly assess and understand the risks and direct and indirect costs involved in third-party relationships.
- Failed to perform adequate due diligence and ongoing monitoring of third-party relationships.
- Entered into contracts without assessing the adequacy of a third party's risk management practices.
- Entered into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers, in order to maximize the third party's revenues.
- Engaged in informal third-party relationships without contracts in place."

Prior to the release of OCC 2013-39, the OCC and the other banking agencies, the OCC, the Federal Reserve Board and the Federal Deposit Insurance Corporation, increased their examination focus on third party risk management, especially relative to consumer compliance risk. This is evidenced by several mortgage consent orders/national mortgage settlements, which held Banks accountable for the actions of their servicers and other foreclosure service providers.

This focus is generally consistent with the Bureau of Consumer Financial Protection's (CFPB or Bureau) release of Bulletin 2012-13, which outlined the CFPB's expectations for business relationships between service providers (i.e., third-parties) and the banks and nonbanks under the CFPB's supervision and enforcement authority. *(Please refer to KPMG Regulatory Practice Letter 12-13.)*

The CFPB guidance references the OCC's Bulletin 2001-47 and generally expects banks and nonbanks to oversee relationships with their service providers to ensure the service providers comply with Federal consumer financial laws and operate in a manner that protects consumers and avoids consumer harm. The CFPB states the legal responsibilities for failure to comply with the laws or to protect consumers, in some cases, may lie with the supervised bank or nonbank in addition to the service provider. Consistent with its guidance, the CFPB also initiated three large enforcement actions during 2012 in which banks were held responsible for the failings of some of their third-party service providers (specifically violations of unfair, deceptive or abusive acts or practices (UDAAP) provisions) and required to pay both restitution and civil money penalties.

Description

Effective Risk Management for Third-Party Relationships

OCC 2013-39 notes that Banks are permitted to outsource some or all of their operating functions to third-party providers but they retain the responsibility to ensure

that the Bank continues to perform in a safe and sound manner and in compliance with applicable laws. Use of third parties reduces management's direct control of activities and may expose Banks to a variety of new risks or actually increase existing risks, especially in the areas of operational risk, compliance risk, reputation risk, strategic risk, and credit risk. The OCC expects Banks to have risk management processes to control for risks from third-party relationships, though it also permits those processes to be scaled based on the risk and complexity of each relationship. Third-party arrangements that involve "critical activities" are expected to have "more comprehensive and rigorous" oversight.

"Critical activities" are defined to include "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.
- Have significant customer impacts.
- Require significant investment in resources to implement the third-party relationship and manage the risk.
- 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 outlines the parameters of an effective risk management process to include: planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, termination plans, oversight and accountability, documentation and reporting, and independent review. Each is briefly described below.

Planning

Senior management is expected to develop a plan to manage all third-party relationships prior to entering into those relationships. The management plan should be commensurate with the risk and complexity of the third-party relationship and relevant considerations should include:

- Identification of inherent risks in the activity to be outsourced.
- An outline of the strategic purposes, legal and compliance aspects, and inherent risks associated with using third parties, and the alignment of such as arrangement with the Bank's overall strategic goals, objectives, and risk appetite.
- Assessment of the complexity of the arrangement, such as the volume of activity, potential for subcontractors, the technology needed, and the likely degree of foreign-based third-party support.
- Analysis of the costs and benefits.
- Impacts to other strategic initiatives.
- Staffing impacts and transition steps needed to initiate and manage the outsourcing process.
- Assessment of the nature of the third-party's interaction with customers.
- Assessment of potential information security implications.
- Contingency plans in the event of contract default or termination.
- Identification of the specific laws and regulations to which the activity is subject.
- Consistency with the Bank's broader corporate policies and practices, including its diversity policies and practices.
- The processes to select, assess, and oversee the third party, including monitoring the third party's contract compliance.
- Board of director approval when critical activities are involved.

Due Diligence and Third-Party Selection

Due diligence should be conducted on all third-parties before selecting and entering into contracts or relationships. The OCC does not consider experience with or prior knowledge of a third-party to be a proxy for an objective, in-depth assessment. Results of third-party due diligence reviews involving critical activities should be presented to the Bank's board of directors. For each prospective third-party, the due diligence review should consider the third-party's:

- Strategies and goals (e.g., business arrangements, service philosophies, employment policies).
- Legal and regulatory compliance (e.g., licensing, expertise, regulatory status).
- Financial condition (e.g., review of audited financial statements).
- Business experience and reputation (e.g., complaint and/or litigation history reference checks).
- Fee structures and incentives.
- Qualifications, backgrounds, and reputation of company principals.
- Risk management (including policies, processes and internal controls).
- Information security.
- Management information systems (including gap analysis for service level expectations).
- Resilience (ability to respond to disruptions or degradations of service).
- Incident reporting and management programs.
- Physical security.
- Human resource management.
- Reliance on subcontractors.
- Insurance coverage.
- Conflicting contractual arrangements.

Contract Negotiation

Management should negotiate a contract with a selected third-party that clearly specifies the rights and responsibilities of each party to the contract. Additionally, board approval of the contract should be obtained before its execution when a third-party relationship will involve critical activities. Contracts should generally address the following:

- Nature and scope of the arrangement (i.e., identify the frequency, content, and format of the service, product, or function provided).
- Performance measures or benchmarks (e.g., complying with regulatory standards or rules).
- Responsibilities for providing, receiving or retaining information, including methods to address failures to adhere to agreed terms, breaches of material thresholds, or changes to provision of the contracted activities.
- The right to audit and require remediation - including provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the Bank's in-house functions to monitor performance with the contract.
- Responsibility for compliance with applicable laws and regulations.
- Costs and compensation.
- Ownership and license – to cover use of the Bank's information, technology and intellectual property, including the Bank's name, logo, trademark and copyrighted materials.
- Confidentiality and integrity.
- Business resumption and contingency plans.

- Indemnification.
- Insurance.
- Dispute resolution.
- Limits on liability.
- Default and termination.
- Customer complaints (e.g., does the Bank or the third-party respond to complaints).
- Subcontracting.
- Foreign-based third party concerns, including choice-of-law covenants and jurisdictional covenants to address potential disputes.
- OCC Supervision – contracts with service providers must stipulate the performance of activities by external parties for the Bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials.

Ongoing Monitoring

The OCC expects a Bank's ongoing monitoring of third-party relationships to cover the list of due diligence activities. Sufficient staff with the necessary expertise, authority, and accountability should be dedicated to oversee and monitor the third party commensurate with the level of risk and complexity of the relationship. Bank employees that directly manage third-party relationships should monitor the third party's activities and performance. Particular attention should be given to the quality and sustainability of the third party's controls, and its ability to meet service-level agreements, performance metrics and other contractual terms, and to comply with legal and regulatory requirements. When appropriate, significant issues or concerns arising from ongoing monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, compliance lapses, and the volume and nature of consumer complaints, should be escalated to management.

Terminations

The extent and flexibility of termination rights may vary with the type of activity. However, Banks should have contingency plans, including bringing activities in-house or identifying an alternate third party, for instances of a contract default or other termination event.

Oversight and Accountability

A Bank's board of directors, senior management, and employees within the lines of businesses (LOBs) who manage the third-party relationships have distinct but interrelated responsibilities 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.

Documentation and Reporting

A Bank should properly document and report on its third-party risk management process and specific arrangements throughout their life cycle. The OCC outlines that such reporting and documentation should typically include:

- A current inventory of all third-party relationships, clearly identifying those relationships that involve critical activities and delineating the risks posed by those relationships across the Bank.
- Approved plans for the use of third-party relationships.

- Due diligence results, findings, and recommendations.
- Analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the Bank.
- Executed contracts.
- Regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements).
- Regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities.
- Regular reports to the board and senior management on the results of independent reviews of the bank's overall risk management process.

Independent Review

Banks should conduct periodic independent reviews on the third-party risk management process, particularly when third parties are involved in critical activities. The Bank's internal auditor or an independent third party may perform the reviews, and senior management should ensure the results are reported to the board. Reviews may include assessing the adequacy of the bank's process for:

- Ensuring third-party relationships align with the bank's business strategy.
- Identifying, assessing, managing, and reporting on risks of third-party relationships.
- Responding to material breaches, service disruptions, or other material issues.
- Identifying and managing risks associated with complex third-party relationships, including foreign-based third parties and subcontractors.
- Involving multiple disciplines across the Bank, as appropriate during each phase of the third-party risk management life cycle.
- Ensuring appropriate staffing and expertise to perform due diligence and ongoing monitoring and management of third parties.
- Ensuring oversight and accountability for managing third-party relationships (e.g., whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority).
- Ensuring that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties.
- Identifying and managing concentration risks that may arise from relying on a single third party for multiple activities, or from geographic concentration of business due to either direct contracting or subcontracting agreements to the same locations.

Management is expected to respond promptly and thoroughly to significant issues or concerns identified by the independent review and to escalate the issues to the board if the risk posed approaches the Bank's risk appetite limits.

Supervisory Review

The OCC expects Bank management to engage in a "robust analytical process" 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. As part of its supervisory review of risk management processes for third-party relationships, OCC examiners will assess the Bank's ability to oversee and manage it third-party relationships and discuss any material risks or deficiencies in the process with Bank's board and senior management. The findings of the review will

be considered when assigning the Bank's CAMELS rating (Federal Financial Institutions Examination Council's (FFIEC) Uniform Financial Institutions Rating System).

The OCC also has the authority to examine, "when circumstances warrant," the functions or operations performed by a third party on a Bank's behalf. Such examinations may evaluate the third-party's: safety and soundness risks; financial and operational viability to fulfill its contractual obligations; compliance with applicable laws and regulations, including consumer protection, fair lending, Bank Secrecy Act/anti-money laundering and OFAC (Office of Foreign Assets Control) laws; and conduct with regard to the unfair or deceptive acts or practices provisions under federal or applicable state law (or the CFPB's UDAAP).

The OCC states that it will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by a Bank or its third party. The OCC has the authority to assess a Bank for a special examination or investigation fee when the OCC examines or investigates the activities of the Bank's third party.

Commentary

As evidenced by the CFPB's 2012 guidance and the related enforcement actions that carried significant restitution and civil money penalty payments, there has been an increase in supervisory scrutiny of third-party relationships, including efforts to strengthen oversight (monitoring, testing and controls), governance (roles and accountability), arrangements (contracts), and selection (risk-based evaluation and streamlining). Accordingly, the OCC's enhanced guidance is not unexpected.

It should be noted that while OCC Bulletin 2013-29 is directed to national banks and Federal savings associations (institutions under OCC supervision authority), it is very likely the other Federal banking regulators will mirror the OCC guidance by updating their own supervisory expectations for third-party risk management or jointly through the Federal Financial Institutions Examination Council (FFIEC).

Unlike CFPB Bulletin 2012-13, the OCC guidance identifies more detailed safety and soundness requirements in addition to Banks' obligation to comply with Federal consumer laws relative to their third-party relationships.

Further, the OCC defines third-parties very broadly, including "any business arrangement between a bank and another entity, by contract or otherwise" and expects Banks to have effective risk management processes for each of these relationships. For many Banks, the number of these arrangements could reach into the hundreds or thousands, including vendors, suppliers, outsource providers (such as IT providers or call centers), joint venture partners, affiliates, professional service firms, business alliance members, contingency arrangement participants, contingent workers, and transaction counterparties. Clearly, the regulatory expectation is that Banks have an effective process to differentiate, categorize and manage their third-party relationships by risk.

Key Takeaways

1. Banks should assess their current third-party risk management processes against the requirements of OCC 2013-29 as well as consider the linkage of the third-party risk management program elements to the bank regulators' overall heightened supervisory expectations for risk management and internal audit (e.g., the OCC's "Get to Strong" principles).

2. Banks should develop plans for executing periodic independent reviews on their third-party risk management process.

Contact us:
This is a publication of KPMG's
Financial Services Regulatory Practice

Contributing authors:
Hugh Kelly, Principal: hckelly@kpmg.com
Greg Matthews, Managing Director: gmatthews1@kpmg.com
Karen Staines, Associate Director: kstaines@kpmg.com

Earlier editions are available at:
http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/regulatory-practice-letters/Pages/Default.aspx