Financial Risk Management

A Regulatory Approach to Third-party Risk Management

February 2014

kpmg.com
Contents

Background 1

Third-party Vendor Risk Management Life Cycle 2
   i. Planning to manage the third-party vendor relationship 3
   ii. Due diligence and third-party selection 3
   iii. Contract negotiations that clearly specify rights and responsibilities 5
   iv. Ongoing monitoring 6
   v. Termination of a third-party relationship 7

Steps to Executing the Risk Management Process 8

In Conclusion 8
Regulators are concerned about risks associated with banks and “non-depository consumer financial service companies” (nonbanks) that use third-party suppliers. They recognize that banks use third parties primarily to (1) outsource internal operations, business lines, and product offerings; (2) make available to their customers products or services that they do not generally provide; and (3) lend their name or regulated status to activities or services conducted by others for a fee. In the case of nonbanks, the Consumer Financial Protection Bureau (CFPB) identifies the primary risk of consumer harm as arising from the use of third parties to (1) make up for resource constraints, (2) develop additional products or services, and (3) provide expertise that would not otherwise be available internally.

A primary objective of the regulators’ examinations and regulations pertaining to third parties is to monitor whether the quality of risk management of third-party relationships is consistent with their degree of risk and complexity. These risks include both risks to the institution’s business and solvency as well as protection of its customers from financial harm.

In part, regulators’ recent concern stems from trends which have been cited as “reinforcing the need” for banks to maintain effective risk management practices around third-party relationships. These trends include banks failing to understand the risks of direct and indirect costs involved in third-party relationships and failing to perform due diligence and ongoing monitoring of third parties. In addition, there is concern about the trend for banks to enter into contracts without assessing third parties’ risk management practices and engaging in informal third-party relationships without a contract. There is also concern about contracts that are detrimental to bank customers and those which have incentives contrary to customer interests.

Additionally, the fact that third parties may not be directly subject to certain banking or financial reporting requirements may leave banks and nonbanks exposed to civil or even potentially criminal penalties. Recurring examples of this are the consent order cases where the servicing arms of several major banks are under increased regulatory scrutiny as a result of third parties whose subservicing and default management practices were not compliant with state foreclosure laws and/or federal regulations and guidelines.

These types of issues have caused regulators to revisit their promulgated guidance and examine other areas where banks and nonbanks may be exposed to similar third-party risks.

As they revisit the guidance, some regulators derive authority to reach out to third parties from the Bank Service Company Act (the Act). When the third party is performing functions of the bank’s internal operations, federal regulators treat these third-party functions as subject to the Act. Under this law, some regulators have asserted a general authority to examine and regulate the functions or operations of a bank’s third-party suppliers as if they were being performed by the bank itself. Others have chosen to state a more direct relationship, providing guidance for whenever there is “any business arrangement between a bank and another entity, by contract or otherwise.”

The legislation and guidance referred to above may not apply to some third parties that are not national banks or federal savings associations. Nevertheless, they should recognize that the Dodd-Frank Wall Street Reform and Consumer Protection Act, in addition to creating the new CFPB, has also created an enforceable jurisdiction for the CFPB that includes “any person that provides a material service to a [bank or nonbank] in connection with offering or provision by the [bank or nonbank] of a consumer financial product or service.”

---

7 Ibid.
8 Ibid.
11 See OCC Bulletin 2013-29. (Defines third-party relationships as including 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 responsibility for associated records. Affiliate relationships are also subject to the Federal Reserve Act as implemented through Regulation W.)
KPMG LLP’s (KPMG) Financial Risk Management practice focuses on providing risk management support services in response to regulators’ third-party guidance. Regulators have outlined five “life cycle” components that should be included in the risk management process, which are included in KPMG’s approach to third-party compliance. They are (1) planning to manage the third-party relationship, (2) due diligence and third-party selection, (3) contract negotiation, (4) ongoing monitoring of the third party, and (5) contingency planning to transition in the case of terminating a third party or bringing a third-party activity in-house.\(^\text{13}\)
i. Planning to manage the third-party vendor relationship

KPMG can make recommendations and bring industry perspectives to bear on aligning third-party policies and procedures with a bank or nonbank’s risk concerns and ultimately with regulatory guidance. During the planning process, senior management should develop a plan to manage the third-party relationship. The plan should:

- Discuss inherent activity risks;
- Outline strategic purpose, compliance, and legal considerations and align them with the bank’s overall strategic goals;
- Assess the complexity of the arrangement (volume, need for subcontractors, technology, foreign or third-party-based support);
- Determine whether the financial benefit outweighs the costs;
- Consider how the third-party relationship could affect the bank’s strategic initiatives;
- Consider how the third-party relationship impacts on bank employees and on third-party employees;
- Outline plans to manage the impact of the third-party relationship on customer confidential information, marketing or franchising, and compliance handling;
- Assess the impact on information security;
- Consider the bank’s contingency plans for transitioning to another third party or bringing the activity in-house;
- Assess specific regulatory requirements that apply to the third-party activity;
- Consider whether the selection of the third party is consistent with the bank’s broader diversity policy;
- Detail how the bank will select, assess, and oversee the third party; and
- Consider whether the third party will be presented to the bank’s board for approval when critical activities are involved.13


ii. Due diligence and third-party selection

Selecting a competent and qualified third party to provide services is critical to good risk management. While regulators do not prescribe a mandatory list of due diligence procedures, the degree of due diligence should depend on the level of risk and complexity of the third-party relationship. Management should conduct due diligence on all potential third parties before selecting and entering into contracts or relationships. Specifically, relying solely on a management’s experience with or prior knowledge of a third party should not be a proxy for an objective in-depth assessment of the third party’s ability to perform an activity. Then, senior management should review the due diligence results to decide whether to proceed with a third-party relationship.
KPMG will review the products and operations that a third party provides and will undertake a gap analysis of potential strengths and concerns. As part of our approach, KPMG also incorporates the following regulator-cited considerations that management should consider when conducting its third-party due diligence, when applicable:

- Overall strategies and goals of the third-party;
- Effective risk management program and internal controls environment;
- Legal and regulatory compliance;
- Experience in implementing and technology supporting the proposed activity;
- Alignment of fee structure and incentives to mitigate inappropriate risk taking;
- Qualifications, backgrounds, and reputations of company principals;
- Adequacy of management and security related to information systems;
- Business resilience planning including continuity, recovery, and contingency plans;
- Physical security;
- Incident-reporting programs and human resource management;
- Reliance on and success in dealing with subcontractors;
- Insurance coverage; and
- Potential conflicts with existing contractual arrangements with other parties.\(^{15}\)

Our approach to due diligence procedures may include:

- Focusing on whether the third party’s own risk management program considers:
  1. Performance monitoring for key actions relevant to the products/operations provided;
  2. Performance monitoring for professional training and legal/regulatory changes specific to the service provided;
  3. How due diligence questions are incorporated into the third party’s onboarding and internal review processes (including Requests for Proposals and Requests for Information);
  4. Tools/sources used to produce products and perform services;
  5. Whether site visits are conducted and how results are incorporated into performance assessments; and
  6. Whether the frequency and degree of performance management is supported by an appropriate assessment of risks.

- Conducting interviews and walkthroughs to obtain an understanding of the following:
  1. Types of information collected;
  2. How the information is vetted and documentation is produced around the process;
  3. Vendor due diligence controls with respect to third-party staffing levels;
  4. Training; and
  5. Work quality and work load balance measures.

- Identifying opportunities for enhancement to the third party’s existing processes and controls.
- Developing or enhancing relevant procedures to remediate identified gaps.

In addition, banks and nonbanks are expected to take steps to ensure that their third parties do not pose unwarranted risks to consumers. These steps should include, at a minimum:\(^\text{16}\)

- Conducting due diligence specifically to verify that the third party understands and is capable of complying with federal consumer financial law;
- Requesting and reviewing policies, procedures, internal controls, and training materials to help ensure proper training and oversight over employees or agents that have consumer contact or compliance responsibilities;
- Including in the third-party contract clear expectations about consumer financial law compliance, enforceable consequences for violating compliance or compliance-related responsibilities such as unfair, deceptive, or abusive acts or practices;
- Establishing internal controls and monitoring to determine whether a third party complies specifically with federal consumer financial law;
- Taking prompt action to address problems when identified, including terminating relationships where appropriate.

iii. Contract negotiations that clearly specify rights and responsibilities

Regulators expect the board of directors and management to ensure that all obligations and expectations related to the third party are clearly defined, understood, and enforceable. When involving critical activities, board approval may be necessary and regulators expect that management will periodically review existing contracts to ensure continued risk controls and legal protections are in place.\(^\text{17}\) The guidance also provides several topics that banks and nonbanks should normally consider when entering into a binding contract. KPMG can provide recommendations, as appropriate, with respect to third-party contracts as they relate to various products and operations. Again, as part of our approach, KPMG takes into consideration the following regulator-cited contract topics, as applicable:\(^\text{18}\)

- Nature and scope of arrangement;
- Performance measures or benchmarks;
- Responsibilities for communicating, receiving, and retaining records and reports;
- Right to audit third parties and their subcontractors and require remediation;
- Right to monitor compliance with applicable laws and regulations;
- Full description of compensation, fees, and calculations for base services, including special fees based on volume or special requests;
- License or statement of how and whether the third party has the right to use the company’s information, technology, and intellectual property/branding;
- Indemnifications holding the third party harmless from liability for the negligence of the bank or nonbank, and vice versa;
- Responsibilities for maintaining appropriate security to protect customer confidentiality and data integrity;
- Insurance coverage maintained by the third party;
- Dispute resolution for the purpose of resolving problems between the bank or nonbank and the third party in an expeditious manner, and whether it should provide that the third party continue to perform during the dispute resolution period;
- Limits on liability in proper proportion to the amount of loss the bank or nonbank might experience as a result of the third party’s failure to perform;
- Default, termination, and continuity planning considerations stipulating what constitutes default, remedies, and opportunities to cure defaults;
- Response to customer complaints;
- Enforceability of the contract on foreign-based service providers;
- Responsibility or liability to the third party related to its use of subcontractors; and
- Regulator examination oversight.\(^\text{19}\)

Our approach to evaluating third-party contract issues may include Contract Completeness. Review current oversight policies as compared to KPMG’s understanding of regulatory expectations. Key tasks can include:

- Through our understanding of various bank and nonbank vendor management programs, KPMG will provide perspective on industry practices and key performance indicators as we discuss approaches to the contract elements noted above.
- Identification of potential gaps in the process.
- Development of or enhancements to relevant procedures to remediate identified gaps.


\(^{17}\) See OCC Bulletin 2013-29.

\(^{18}\) Ibid.

iv. Ongoing monitoring

Once a third party enters into an agreement with a bank or nonbank, the regulators expect management to provide staff with enough expertise to oversee the third party. Both the bank or nonbank and the third party are expected to have created processes for reporting to management and complying with consumer financial law. In addition, the third party should have processes for monitoring the quality and sustainability of its controls and the ability to meet service-level agreements (SLAs), performance metrics on other contract terms, and regulatory compliance requirements. Because the risks and terms of a third-party agreement may change over time, management should ensure that its ongoing monitoring adapts accordingly.21

KPMG can work with the bank, nonbank, or third parties to facilitate reviews and/or audits conducted and help the third party troubleshoot and align its processes and methodologies with bank or nonbank monitoring. In order to scale our approach, we can:

- Evaluate:
  1. Terms/conditions with regard to performance reviews, including escalation of issues;
  2. How third parties assess their performance on a periodic basis (including on-site visits, oversight committees/management boards, issues reporting, testing, and issues remediation);
  3. How third parties rate performance and whether current rating system appropriately considers timeliness, competence, and compliance with all applicable legal requirements;
  4. What drives the frequency and depth of third-party reviews and whether drivers are appropriately risk-based; and
  5. Service levels against which performance is tracked, monitored, and reported.

- Identify and document potential gaps in third-party oversight and reporting processes.

- Develop or enhance procedures to remediate identified gaps.

- Review processes for evaluating the third party’s approach to complaint tracking, follow-up, escalation (if needed), resolution, and reporting.

KPMG can also work with third parties to align and troubleshoot their management reporting processes with those required by their banking and nonbanking clients and regulators. Regulators have provided the following key areas of consideration for ongoing monitoring and program oversight, as applicable:22

- Evaluate the third party’s business strategy and reputation for conflicts of interest and impact on SLAs or contract obligations.
- Review compliance with legal or regulatory requirements to determine if there are licensing or registration requirements to ensure the third party can legally perform its services.
- Evaluate the third party’s financial condition.
- Evaluate the third party’s information technology or management of information technology.
- Evaluate the process for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches.
- Review the adequacy and adherence to the third party’s policies relating to internal controls and security issues.
- Review the third party’s business resumption contingency planning and testing.
- Assess the effect of any changes in key third-party personnel and ability to retain essential knowledge necessary for maintaining the relationship.
- Assess reliance and exposure to performance of subcontractors, location of subcontractors, and the ongoing monitoring and control testing of subcontractors.
- Determine whether agreements with other entities may interfere or conflict with the third party such that it would impact or present certain risks to management.
- Review customer complaints about the products and services provided by the third party and the resolution or remediation related to the complaints.

21 Ibid.
22 Ibid.
v. Termination of a third-party relationship

The regulators recognize that a bank or nonbank may terminate a third-party relationship for a variety of reasons. Those reasons may include expiration or satisfaction of a contract, desire to transition activity to another third party, desire to bring the activity in-house or discontinue it entirely, or a breach of contract by the third party. Management should develop a plan to efficiently transition to another third party or bring in-house activities in the event of third-party default or termination. This plan should cover:

- Time frame and resources required to transition the activity;
- Risks associated with data retention, destruction, and system connectedness;
- Handling of joint intellectual property developed; and
- Reputational concerns if the termination occurs as a result of the third party’s inability to meet expectations or breach.

KPMG can work with banks and nonbanks to develop a transitional plan specific to the level of risk and complexity of activities that the third party is providing.

---

24 Ibid.
To further address their concerns, regulators have specified steps that should be performed throughout the risk management life cycle. KPMG can work with banks, nonbanks, or third parties to troubleshoot the different levels of management operations and processes required for these steps. The guidance provides that throughout the life cycle there should be:  

- Clear assignment of roles and responsibilities of management to manage the third-party relationship and integrate the third-party risk management process with the enterprise risk management framework,
- Proper documentation and reporting, and
- Independent reviews of the third-party risk management processes to align with bank strategy and effectively manage the third-party relationship.

Specifically, the guidance provides that the board of directors is responsible for ensuring that an effective process is in place to manage third-party relationships. It should approve bank policies that govern third-party risk management and approve management’s plans for using third parties to provide critical activities. In addition, for a third party providing critical activities, the board should review due diligence results and management recommendations and approve the related contracts.

Additionally, senior management should develop and implement the bank’s third-party risk management process. Management should establish the bank’s risk and governance policies incorporating the risk management life cycle components, reporting results to the board. Management is responsible for ensuring that independent reviews are conducted and for analyzing their results to determine whether the bank should adjust its third-party risk management process, including policy, reporting, resources, expertise, and controls. It should hold employees who manage the direct third-party relationships accountable, terminate arrangements when necessary, and oversee enterprise-wide risk management and reporting of third-party relationships.

Regulators have also provided guidance that bank employees who directly manage third-party relationships should perform due diligence and ensure ongoing compliance with contract terms, service-level agreements, and regulatory requirements. Employees should execute regular testing of bank controls and execute responses to material weaknesses. They should conduct the independent reviews to ensure that expectations in each phase of the risk management life cycle are being met by third parties. These responsibilities should be documented along with an inventory of all third-party relationships that should correspond to approved plans for the use of third parties. Then, the employees should also have processes to escalate significant issues to senior management and processes to provide regular reports to the board and senior management on the results of internal control testing, ongoing monitoring, and independent reviews.

KPMG is one of the largest professional services firms in the world, providing a range of financial risk advisory, technology assurance, and performance improvement services to a wide array of clients, including numerous federal and state government agencies, banking supervisors, leading financial services companies, and government-sponsored enterprises.

We can leverage these valuable insights and experiences into the application of third-party risk management principles where appropriate, and will involve KPMG subject matter professionals when circumstances require additional knowledge of specialized financial or technical services matters.

---

26 Ibid.
27 Ibid.
28 Ibid.