KPMG
cutting through complexity

Third Party Risk Management in the New Regulatory Environment

kpmg.com

Vendor Risk Management in the New Regulatory Environment

Background

Regulators are concerned about risks associated with banks and "nondepository consumer financial service companies" (nonbanks) that use third-party vendors.[1] They recognize that banks use third-party vendors primarily to (1) outsource internal operations, (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.[2] In addition, for nonbanks, one regulator has begun to focus on the risk of harm to consumers based on the use of third-party vendors to (1) make-up for resource constraints, (2) develop additional products or services, and (3) provide expertise that would not be otherwise available internally.[3]

A primary objective of the regulators' examinations and regulations pertaining to third-party vendors is to determine whether the financial institution's third-party relationships create more risk than the financial institution can identify, monitor, manage, or control. These risks include both risks to the financial institution's business and solvency as well as the financial institution's protection of its customers from financial harm.[4]

In part, regulators' recent concern stems from the fact that third-party vendors may not be directly subject to certain banking or financial reporting requirements. The third-party vendors' lack of accountability to regulators may leave banks and nonbanks exposed to civil or even potential criminal penalties.[5] As a recent example, the servicing arms of several major banks are under increased regulatory scrutiny and in some cases subject to regulatory consent orders as a result of third-party vendors 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 vendor risks.

As they revisit the guidance, many regulators have stated that they derive authority to reach out to third-party vendors from the Bank Service Company 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.[6] Under this law, regulators have reasserted a general authority to examine and regulate a bank's third-party vendor functions or operations as if they were being performed by the bank itself.

While some third-party vendors may correctly understand that the Bank Service Company Act may apply directly to them, they should also recognize that the Dodd-Frank Act, in addition to creating the new Consumer Finance Protection Bureau (CFPB), has also granted the CFPB jurisdiction over "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]

---

[1] See generally OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," available at: http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html. See also CFPB Bulletin 2012-13, Service Providers," April 13, 2012 available at: http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf.

[2] See generally OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," available at: http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html.

[3] See CFPB Bulletin 2012-13

[4] See CFPB Bulletin 2012-13

[5] See Bank Secrecy Act/Anti-Money Laundering Examination Manual: Third-Party Payment Processors – Overview, Federal Financial Institutions Examination Council available at: http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_063.htm.

[6] See Bank Service Company Act (12 U.S.C. 1867(c)) available at: http://www.gpo.gov/fdsys/pkg/USCODE-2009-title12/pdf/USCODE-2009-title12-chap18-sec1867.pdf.

[7] See CFPB Bulletin 2012-13

THIRD-PARTY VENDOR RISK MANAGEMENT PRINCIPLES

To address their concerns, regulators have issued guidance to financial institutions providing a framework for managing risks related to third-party business relationships. The guidance provides general risk management principles which are expected to be adapted to the individual risk profile of the bank or nonbank. In general, the board of directors and senior management retain accountability and, therefore, must scale these principles according to the magnitude and criticality of the third-party provided product or services.

In addition, the CFPB has determined that financial institutions under its supervision may be held responsible for the actions of the companies with which they contract; and expects that supervised financial institutions have an effective process for managing the risks of service provider relationships. Financial institutions need to ensure that business arrangements with service providers do not present unwarranted risks to consumers.

KPMG LLP (KPMG) provides risk management support services in response to banks' and nonbanks' needs arising out of regulators' guidance on third-party vendor risk management. In summary, these are:

- Risk assessment
- Third-party due diligence
- Contracting
- Continued oversight.

(See Table 1.)

Table 1	Risk Assessment	Third- Party Due Diligence	Contracting	Continued oversight
Key activities in a vendor risk managment program	■ Develop a risk assessment framework that stratifies vendors based on their risk to the organization and consistency with overall strategic objectives	■ Prior to on-boarding a new vendor, conduct a thorough assessment of the vendor's capability to deliver the services expected in line with the organization's expectations	■ Execute contracts that minimize the risk of nonperformance and confirm the appropriate scope of those contracts	■ Review vendors on a regular basis to reconfirm the organization's understanding of the risk the vendor poses and the performance management process
Consumer protection focus	■ Identification of consumer-facing and consumer-impacting vendors ■ Clear articulation of applicable laws to each product, and at each stage of the product life cycle ■ Mapping of vendors and laws and regulations that are applicable to them	■ Assessing vendors prior to them commencing work to determine whether they increase the risk of consumer harm factoring in the inherent risk of consumer harm given the products and services that will be outsourced and the control environment currently in place	■ Incorporating terms into the contract to allow the client to assess the control environment in place at the vendor on an ongoing basis	■ Identification of regulatory changes and incorporation of those into the assessment questions used to review a vendor ■ Obtaining information from the vendor to allow the client to assess the control environment as part of the assessment

[8] OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," available at: http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html. See also: FDIC Financial Institution Letters FIL-44-2008, "Third-Party Risk: Guidance for Managing Third-Party Risk," available at: http://www.fdic.gov/news/news/financial/2008/fil08044.html. See generally: "FDIC Supervisory Insights: Managing Risks in Third-Party Payment Processor Relationships," by Michael B. Bernardo et al., Summer 2001, available at: http://www.fdic.gov/regulations/examinations/supervisory/insights/sisum11/managing.html. FDIC Financial Institution Letters FIL-127-2008, "Guidance on Payment Processor Relationships," available at: http://www.fdic.gov/news/news/financial/2008/fil08127.html. "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks," Federal Reserve Bank of New York, October 1999 available at: http://www.ny.frb.org/banking/circulars/outsource.pdf. See also CFPB Bulletin 2012-13, which referenced the OCC 2001-47.

I – RISK ASSESSMENT

KPMG can make recommendations and provide industry perspective to assist in aligning third-party policies and procedures to a bank or nonbank's risk concern in light of the recent regulatory guidance. The risk assessment process can be characterized by four subcomponents that financial institutions should consider when applicable. These components are:

- Integration assistance with overall strategic objectives and business planning
- Assistance to manage and oversee the transition to a third-party provided operation
- Cost/Benefit relationship recommendations considering long-term stability and viability
- Recommendations concerning managing customer expectations with respect to new products and services.[9]

In addition, banks and nonbanks are expected to take steps to ensure that their third-party vendors do not pose unwarranted risks to consumers. These steps should include, at a minimum:[10]

- Conducting due diligence specifically to verify that the third-party vendor understands and is capable of complying with federal consumer financial law
- Requesting and reviewing policies, procedures, internal controls, and training materials to ensure proper training and oversight over employees or agents who have consumer contact or compliance responsibilities
- Including in the vendor contract clear expectations about consumer financial law compliance and 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 vendor complies specifically with federal consumer financial law
- Taking prompt action to address problems when identified, including terminating relationships where appropriate.

[9] See OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," available at: http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html. See also: FDIC Financial Institution Letters FIL-44-2008, pg. 4, "Third-Party Risk: Guidance for Managing Third-Party Risk," available at: http://www.fdic.gov/news/news/financial/2008/fil08044.html. See also: "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks," pg. 8, Federal Reserve Bank of New York, October 1999, available at: http://www.ny.frb.org/banking/circulars/outsource.pdf.

[10] See CFPB Bulletin 2012-13

II – THIRD-PARTY VENDOR DUE DILIGENCE

Selecting a competent and qualified third-party vendor to provide services is critical to risk management, and regulators have highlighted it as another cornerstone component to a functioning risk management process. While regulators do not prescribe a mandatory list of due diligence procedures, they do expect compliance with consumer financial laws and they do provide a robust list of considerations and, notably, a general expectation that the depth and breadth of a financial organization's due diligence should increase as the complexity of services or reliance on the third-party vendor increases. As part of our approach, KPMG also incorporates the following regulator-cited considerations, when applicable:

- Experience in implementing and supporting the proposed services/product
- Audited financial statements of the third party and its significant principals
- Business reputation, complaints, and litigation
- Qualifications, backgrounds, and reputations of company principals
- Internal controls environment and audit coverage
- Adequacy of management information systems
- Business continuity, recovery, and contingency plans
- Technology recovery testing efforts
- Cost of development, implementation, and support
- Reliance on and success in dealing with subcontractors
- Insurance coverage.[11]

Examples of our approach to financial organizations' due diligence procedures may include:

- Focusing on whether the vendor's own performance management program considers:
  - Performance monitoring for performing key actions relevant to the products/services provided to the financial organization
  - Performance monitoring for professional training and legal/regulatory changes specific to the service provided
  - How due diligence questions are incorporated into the vendor's on-boarding and internal review processes (including RFPs and RFIs)
  - Tools/sources used to produce products and perform services
  - Whether site visits are conducted and how results are incorporated into performance assessments
  - 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:
  - Types of information collected
  - How the information is vetted and documentation is produced around the process
  - Vendor due diligence controls with respect to third-party staffing levels
  - Training
  - Work quality and work load balance measures
- Identifying opportunities for enhancement to the vendor's existing processes and controls
- Developing or enhancing relevant procedures to remediate identified gaps.

III – WRITTEN CONTRACTS FOR DUTIES, OBLIGATIONS, AND RESPONSIBILITIES

Regulators expect the bank and nonbank board of directors and management to ensure that all obligations and expectations related to the third-party vendor are clearly defined, understood, and enforceable. Besides specific scope of the products and operations to be provided, the guidance also provides several topics that banks and nonbanks should normally consider when entering into a binding contract. KPMG can provide recommendations in relation to the products and services to be included in third-party vendor contracts. Again, as part of our approach, we include in our considerations the following regulator-cited contract topics when applicable:

- Scope of arrangement
- Performance measures or benchmarks
- Responsibilities for communicating information to management information
- The right to audit third parties and their subcontractors and SAS 70 reviews
- Cost/compensation and payment terms
- Ownership and licensing of the bank/nonbank's data, hardware and software, system; documentation; and intellectual property, such as the bank/nonbank's name, logo, trademark, and copyrighted material
- Information protection, confidentiality, and security

[11] This list has been included for example purposes and, as regulation evolves; is not meant to be all inclusive. See OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," available at: http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html. See also: FDIC Financial Institution Letters FIL-44-2008, pg. 6, "Third-Party Risk: Guidance for Managing Third-Party Risk," available at: http://www.fdic.gov/news/news/financial/2008/fil08044.html

- Business continuity and contingency plans for the business function in the event of problems affecting the third party's operations
- Indemnifications holding the third party harmless from liability for the negligence of the bank or nonbank, and vice versa
- Insurance coverage maintained by the third-party vendor
- 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 and termination considerations stipulating what constitutes default, remedies, and opportunities to cure defaults
- Response to customer complaints
- Enforceability of the contract on foreign-based service providers
- Regulator examination oversight.[12]

Examples of our procedures for evaluating third-party vendor 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 can 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.

IV – CONTINUING OVERSIGHT AND MONITORING

Once a third party vendor enters into an agreement with a bank or nonbank, the regulators expect the bank or nonbank management to provide staff with enough expertise to oversee the third-party. Both the bank or nonbank and the third party vendor are expected to have created processes for reporting to management and complying with consumer financial law and regulations. KPMG can work with third-party vendors to facilitate reviews and/or audits conducted by the financial institution and help the third-party vendor troubleshoot and align its processes and methodology with financial institution monitoring.

In order to scale our approach, our approach can include:

- Evaluating:
  - Terms/conditions of agreements with regard to performance reviews, including escalation of issues
  - How third-party vendors assess their performance on a periodic basis (including on-site visits, oversight committees/ management boards, issues reporting, testing, and issues remediation)
  - How third-party vendors rate performance and whether current rating system appropriately considers timeliness, competence, and compliance with all applicable legal requirements
  - What drives the frequency and depth of third-party vendor reviews and whether drivers are appropriately risk-based
  - Service levels against which performance is tracked, monitored, and reported
- Identifing and document potential gaps in third-party oversight and reporting processes
- Developing or enhancement to procedures to remediate identified gaps
- Reviewing processes for evaluating the third-party vendor's approach to complaint tracking, follow-up, escalation (if needed), resolution, and reporting.

Regulators have provided guidance that financial institutions should perform monitoring related to the following key topic areas:

- Financial condition and risk management practices of the third-party vendor
- Internal controls around compliance, contingency planning, quality assurance, and personnel changes
- Assessments of quality of service and support
- Documentation.[13]

KPMG can align and troubleshoot management reporting processes to those required by banking and nonbanking clients and regulators. Within the key topic areas outlined above, regulators have also provided the following performance monitoring and program oversight components, as appropriate:[14]

- Evaluate the overall effectiveness of the third-party vendor relationship and the consistency of the relationship with the financial institution's strategic goals
- Review any licensing or registrations to ensure the third-party vendor can legally perform its services

[12] This list has been included for example purposes and as, regulation evolves is not meant to be all inclusive. See OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles" available at: http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html. See also: FDIC Financial Institution Letters FIL-44-2008, pg. 6, "Third-Party Risk: Guidance for Managing Third-Party Risk," available at: http://www.fdic.gov/news/news/financial/2008/fil08044.html. See also "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks," pg. 15, Federal Reserve Bank of New York, October 1999, available at: http://www.ny.frb.org/banking/circulars/outsource.pdf.

[13] See OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," available at: http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-47.html. See generally: FDIC Financial Institution Letters FIL-44-2008, pg.9-10,"Third-Party Risk: Guidance for Managing Third-Party Risk," available at: http://www.fdic.gov/news/news/financial/2008/fil08044.html.

[14] See id.

- Evaluate the third-party vendor's financial condition at least annually; financial review should be as comprehensive as the credit risk analysis performed on the institution's borrowing relationships; audited financial statements should be required for significant third-party relationships
- Review the adequacy of the third-party vendor's insurance coverage
- Review the third-party vendor's financial obligations to others and make observations as to their performance
- Review audit reports or other reports of the third-party vendor, and follow up on any needed corrective actions
- Review the adequacy and adherence to the third-party vendor's policies relating to internal controls and security issues
- Monitor for compliance with applicable laws, rules, and regulations
- Review the third-party vendor's business resumption contingency planning and testing
- Assess the effect of any changes in key third-party vendor personnel involved in the relationship with the financial institution
- Review reports relating to the third-party vendor's performance in the context of contractual requirements and performance standards, with appropriate follow-up as needed
- Assess the adequacy of any training provided to employees of the financial institution and the third-party vendor
- Review testing programs for third-party vendors with direct interaction with customers
- Review customer complaints about the products and services provided by the third-party vendor and the resolution of the complaints
- Meet as needed with representatives of the third-party vendor to discuss performance and operational issues.

KPMG can bring industry-leading expertise to bear, for banks and other financial institutions, and for their contractors and suppliers, to ensure that regulatory concerns about third-party vendor risk are fully satisfied (see Table 2)

Table 2	Risk Assessment	Financial Institutions Due Diligence	Contracting	Continued oversight
Financial institutions	KPMG can assist by: ■ Working to map your regulatory inventory to products and their life cycle ■ Building a set of risk assessment questions allowing vendors to be incorporated into the overall vendor risk management program ■ Enhancing the vendor risk management program to include a consumer protection lens and sound operating risk principles.	KPMG can assist by: ■ Developing questions to allow the financial services company to assess the vendor based on products/processes that will be outsourced. ■ Developing internal controls framework specific to a vendor or class of vendors	KPMG can assist by: ■ Reviewing contract language and identifying components to incorporate	KPMG can assist by: ■ Developing detailed tests/checklists to assess vendors and their information ■ Conducting specific on-site work in a co-source manner ■ Preparing information requests for vendors
Third parties	KPMG can assist by: ■ Preparing you for a detailed risk assessment by a client through a gap assessment ■ Assisting you to enhance your compliance program to manage regulatory compliance risks ■ Assistance in tailoring your products and services to incorporate regulatory compliance.	KPMG can assist by: ■ Preparing you for a detailed risk assessment by a client through a gap assessment ■ Assisting you to enhance your compliance program to manage regulatory compliance risks ■ Assistance in tailoring your products and services to incorporate regulatory compliance	KPMG can assist by: ■ Assistance in tailoring your products and services to incorporate regulatory compliance	KPMG can assist by: ■ Preparing responses to clients in connection with ongoing data requests as part of the risk assessment ■ Assisting you to enhance your compliance program to manage regulatory compliance risks

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.

Contact us

Carolyn Greathouse
Managing Director
Financial Services Regulatory
636-587-2844
cgreathouse@kpmg.com

Jeffrey P. Hulett
Managing Director
Credit Risk
703-286-6695
jhulett@kpmg.com

Hugh Kelly
Principal
Financial Services Regulatory
202-533-5200
hckelly@kpmg.com

Amy Matsuo
Principal
Financial Services Regulatory
919-380-1509
amatsuo@kpmg.com

Greg Matthews
Managing Director
Financial Services Regulatory
201-621-1156
gmatthews1@kpmg.com

Mark A. Twerdok
Partner
Credit Risk
412-232-1599
mtwerdok@kpmg.com

kpmg.com

NDPPS 150938