Third party risk management: Friend or foe?

Leah M. Hamilton, Chief Compliance Officer
What You Will Learn:

- Vendor Management
  - Why use?
  - Potential risks
  - Compliance management
  - Risk assessment
  - Due diligence
  - Contract structuring and review
  - Board and management oversight
Vendor Management

Why use third parties?

- Attain strategic objectives
- Increasing revenues
- Reduce costs
- Access greater expertise or efficiency
- Enhance competitiveness
- Provide diversification
- Strengthen the safety and soundness CMS
Vendor Management

Challenges posed

- Still responsible for activity performed to same extent as if performed by the institution
- Expectation to have a clearly defined system of risk management controls built into CMS, S/S, and IT management systems governing compliance operations, including controls over activities conducted by affiliates and third party vendors
  - Identify and control risks arising from such relationships
  - Does not relinquish responsibility of Board and management
Vendor Management

- To perform functions on behalf of the institution
- To provide products and services institution doesn’t originate
- To "franchise" the institution's attributes
  - Institution lends its name or regulated entity status to products and services originated by others or activities predominantly conducted by others
Common third party arrangements include, but are not limited to:

- Credit card programs (e.g., cash-secured, affinity)
- Payday lending and other alternative credit programs
- Debit card programs;
- Rewards programs
- Deposit taking or affinity relationships;
- Overdraft payment programs
- Refund anticipation loans,
- Audit programs of third party relationships,
- Broker-dealer relationships for brokerage services,
- Mortgage brokerage services,
- Automobile dealer relationships,
- Flood determination services, and
- Reverse mortgage program
Potential Risks Arising from Third Party Relationships

- Strategic
- Reputation
- Compliance
- Credit
- Operational
- Transaction
Compliance risk

- Arises from violations of laws, rules, or regulations, or from noncompliance with internal policies or procedures or with institution's business standards
- Exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, policies, or ethical standards
- Liability could potentially extend to institution
- Exacerbated when inadequate oversight, monitoring or audit functions
Potential Risks

- **Strategic risk**
  - Arises from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with institution’s strategic goals
    - Achieve strategic goals
    - Provide an adequate return on investment

- **Operational risk**
  - Risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events
  - Integrated internal processes

- **Transaction risk**
  - Arising from problems with service or product delivery
    - Failure to perform as expected by customers or the institution due to reasons such as inadequate capacity, technological failure, human error, or fraud
    - Lack of an effective business resumption plan and appropriate contingency plans
    - Weak control over technology may result in threats to security and the integrity of systems and resources
    - Unauthorized transactions or the inability to transact business as expected
Potential Risks

- Credit risk
  - Risk that a third party, or any other creditor necessary to the third party relationship, is unable to meet the terms of the contractual arrangements or to otherwise financially perform as agreed
  - Basic form is the financial condition of the third party itself
  - Appropriate monitoring of third party activity to understand credit risk and remains within board-approved limits

- Reputational risk
  - Arises from negative public opinion
    - Dissatisfied customers, interactions not consistent with institution's policies, inappropriate recommendations, security breaches resulting in disclosure of customer information, and violations of law and regulation
    - Any negative publicity involving the third party, whether or not the publicity is related to institution's use of the third party

- Other risks
  - Liquidity, interest rate, price, foreign currency translation, and country risks
Effective Third Party Risk Compliance Management

(4) principal elements:

- Risk Assessment
  - Assess risks and options for controlling third party arrangements

- Due Diligence in Selecting a Third Party
  - Select a qualified entity to implement the activity or program

- Contract Structuring and Review
  - Ensure specific expectations and obligations of both the institution and the third party are outlined in a written contract prior to entering into the arrangement
    - Should serve as a map to the relationship and define its structure

- Oversight
  - Review operational and financial performance of third party activities on an ongoing basis
Compliance Management System should incorporate (as applicable and as may be appropriate):

- Identification of “significant” third party relationships;
- Policies and procedures, internal controls, training, monitoring, and internal and external auditing procedures associated with third party relationships are consistent and have ongoing compliance with all applicable consumer protection laws and regulations;
- Activities conducted through third parties are compliant with applicable consumer protection laws, fair lending regulations, and internal policies; and
- Appropriate corrective action when third party risk issues are identified or deficiencies are noted.
Risk Assessment

- Fundamental to the initial decision of whether or not to enter into a third party relationship

- Areas to consider:
  - Ensure that the proposed third party relationship is consistent with strategic planning and overall business strategy
  - The strategic risk given size, resources, capacity, and number of employees
  - Benefits, costs, legal aspects, and the potential risks associated with the third party under consideration
  - Perform a risk/reward analysis, comparing the proposed third party relationship to other methods of performing the activity or product offering, including the use of other vendors or in-house staff
    - Integral to overall strategic planning
    - Performed by senior management and reviewed by the board or an appropriate committee
    - Staff have the requisite knowledge and skills to adequately perform the risk analysis
Additional areas to consider

- Certain aspects of the risk assessment phase may include use of internal or external auditors, compliance officers, technology officers, and legal counsel

- Identify performance criteria, internal controls, reporting needs, and contractual requirements that would be critical to the ongoing assessment and control of specific identified risks

- Review whether third party’s activities could be viewed as predatory, discriminatory, abusive, unfair, or deceptive to the customers (both commercial and consumer)

- Ensure ability to provide adequate oversight and management of the proposed third party relationship on an ongoing basis

- Ensure a process in place for elevating new or significant third party relationships and issues to the board and appropriate committee for review and approval
Risk Rating

- Risk rate annually as part of third party monitoring
  - High Risk
    - Provides mission critical services
    - Direct access to nonpublic or confidential customer information and account processing functions
    - All foreign based service providers should be designated High Risk
  - Moderate Risk
    - Provides non-mission critical services
    - Direct access to nonpublic or confidential customer information in a non-account processing function capacity
  - Low Risk
    - No direct access to nonpublic or confidential customer information
    - Any Third party not formally categorized as High or Moderate Risk is presumed to be Low Risk
Due Diligence in Selecting a Third Party

- Audited financial statements, annual reports, Securities and Exchange Commission filings, and other available financial information
- Significance of the proposed contract on the third party’s financial condition
- Experience and ability in implementing and monitoring the proposed activity
- Business reputation, including any complaints filed
- Span of business operations in which the third party is engaged
- Qualifications and experience of the company’s principals
- Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies
- Existence of any significant complaints or litigation (past and pending), or supervisory actions against the company or its owners or principals
Due Diligence

- Ability to perform the proposed functions using current systems or the need to make additional investment
- Use of other parties or subcontractors by the third party
- Scope of internal controls, systems and data security, privacy protections, and audit coverage
- Business resumption strategy and contingency plans
- Knowledge of and background and experience with consumer protection and civil rights laws and regulations
- Underwriting criteria
- Adequacy of management information systems
- Insurance coverage
- Marketing materials to determine how the Institution’s name will be associated with the product
- Websites
- Vendor and Institution management responsibilities
Due Diligence

Other considerations:

- Probe for intangibles
  - Business strategies and goals
  - Human resources policies
  - Service philosophies
  - Quality initiatives
  - Policies for managing costs and improving efficiency.

- Culture, values, and business styles
Contract Structuring and Review

- Scope
- Cost/Compensation
- Performance Standards
- Reports
- Audit
- Confidentiality and security
- Customer complaints
- Business resumption and continuity plans
- Default and termination
- Dispute resolution
- Ownership and license
- Indemnification
- Limitations on liability
- Foreign-based service providers
- Subcontracting
Performance Monitoring

- Evaluate the overall effectiveness of the third party relationship and the consistency of the relationship with the Institution's strategic goals
- Review any licensing or registrations to ensure the third party can legally perform its services
- Evaluate the third party'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's insurance coverage
- Ensure that the third party's financial obligations to others are being met
- Review audit reports or other reports of the third party, and follow up on any needed corrective actions
- Review the adequacy and adherence to the third party's policies relating to internal controls and security issues
- Monitor for compliance with applicable laws, rules, and regulations
Performance Monitoring

- Review the adequacy and adherence to the third party's policies relating to internal controls and security issues
- Monitor for compliance with applicable laws, rules, and regulations
- Review the third party's business resumption contingency planning and testing
- Assess the effect of any changes in key third party personnel involved in the relationship with the Institution
- Review reports relating to the third party's performance in the context of contractual requirements and performance standards, with appropriate follow-up as needed
- Determine the adequacy of any training provided to employees of the Institution and the third party
- Administer any testing programs for third parties with direct interaction with customers
- Review customer complaints about the products and services provided by the third party and the resolution of the complaints
- Meet as needed with representatives of the third party to discuss performance and operational issues
Outsourcing creates risk that vendor's operations can be disrupted and might affect the institution for the services vendor provides.

- To mitigate, must ensure vendor has a prudent business recovery plan in place that is reviewed on an ongoing basis.
- Must address the risk that vendor may not perform satisfactorily:
  
  “In the face of unsatisfactory responsiveness, an institution's options include changing service providers, returning the activity to the institution, or sometimes even exiting the business.”

- Such options are costly and problematic and are usually taken only as a last measure after reasonable efforts to resolve the issues with the vendor.

- Consider mitigating risk by starting out small or limiting the number of services provided by the vendor.
Board and Management Oversight

- Board and senior management is ultimately responsible for its third party relationships
  - Maintain adequate oversight
    - Allocate sufficient qualified staff to monitor significant third party relationships and provide the necessary oversight
  - Maintain adequate quality control over products and services provided
Summary Best Practices

- Implement a comprehensive Vendor Management Program
  - Establish third party risk management program to address activities and relationships
  - Conduct due diligence commensurate with the risk in selection process
  - Ensure relationship is governed by written contract
  - Ensure institution’s ability to fulfill obligations to both customers and regulators
  - Ensure mandatory protection of confidential information
- Develop and maintain contingency business plans, including back up facility testing
FDIC: FIL 50-2016, Proposed Guidance for Third-Party Lending

See, e.g., CFPB Bulletin 2012-03, Service Providers (Apr. 13, 2012),


FDIC FIL 44-2208, Managing Third-Party Risk (June 6, 2008),

FDIC Examination Manual, Third Party Risk (Dec. 2102),

NCUA Letter 07-CU-13, Evaluating Third Party Relationships (Dec. 2007),


Questions?