Vendor Management Best Practices

Presented by:

Raji Sathappan, MBA, CRCM, CISA, CAMS

FMS East Coast Regional Conference

September 2015

MERCADIEN

Certified Public Accountants | Consultants | Wealth Management | Technology

Third Parties

Who?

- Vendors
- Suppliers
- Outsourcing Providers
- Joint Ventures
- Affiliates
- Contingent Workers
- Contingent Deals
- Alliances

What?

- Services
- Access
- Products
- Goodwill
- Processes
- Market Presence
- Intellectual Property
- Regulatory Req.
- Off-shore

How?

- On-site
- Off-site
- Continuous
- Integrated
- Periodic
- ‘Cloud’

MERCADIEN

Agenda

- Regulatory Guidance
- Risk Assessment
- Vendor Management Life Cycle
- Tips and Tricks

MERCADIEN

Regulations and Guidelines

- **Federal Reserve Supervisory Letter SR 13-19/CA 13-21**, Guidance on Managing and Outsourcing Risk, 12/13.
- **OCC Bulletin 2013-29**, Third-Party Relationships, 12/13.
- **CFPB Bulletin 2012-03**, Service Providers, 4/12.
- **Regulatory Notice 11-14**, Proposed by FINRA Rule 3190 Use of Third-Party Service Providers, 5/11.
- **Federal Financial Institutions Examination Council**, Outsourcing Technology Services, 6/04.
- **Prudential Regulation Authority**, SYSC Chapter 8 Outsourcing, 1/13.
- **Financial Conduct Authority**, Consideration for firms thinking of utilizing third-party technology (off-the-shelf) banking solutions, 7/14.

MERCADIEN

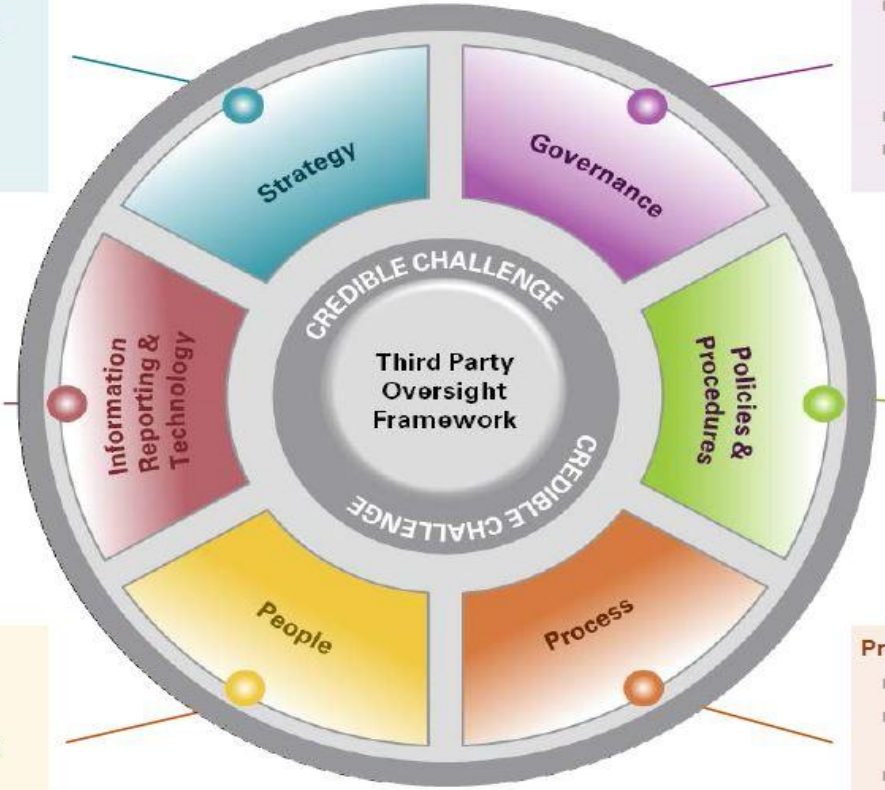
View From Above – *Framework is Key*

Strategy
- Mission and Objectives
- Align Third Party Use to Risk Appetite
- Management of operating expenditures

Governance
- Oversight structure/ committees (i.e., Board, Enterprise Risk Management, Operations Risk)
- Tone & Culture
- Structure and Organization

Information Reporting & Technology
- Dashboards/Reports
- Key Risk Indicators (KRIs)
- Key Performance Indicators (KPIs)
- Process Automation

Policies and Procedures
- Standard Setting
- Policy Management



People
- Roles & Responsibilities
- Skills & Training
- Performance Management & Compensation

Process
- Planning
- Risk Assessment, Due Diligence and Selection
- Contracting
- Monitoring & Testing
- Off-Boarding

Overview - *Regulatory Guidance*

- FIL 44-2008 "Guidance for Managing Third-Party Risk" concerning due diligence and maintenance of oversight, as well as identifying and controlling risk related to non--affiliated third-party relationships.

- Federal Reserve via Supervisory Letter 13-19, "Guidance on Managing Outsourcing Risk," to ensure vendor management policies and procedures are appropriately addressing this risk 12/13.

- FFIEC IT Handbook on Outsourcing Technology Services 6/04.

MERCADIEN

Summary of Guidance

- Provides a general framework that boards of directors and senior management may use to provide appropriate oversight and risk management of **significant third-party relationships**.

- A third-party relationship should be considered significant if the:
  - Institution's relationship with the third party is **new** or involves **implementing new bank activities** or has a **material effect on the institution's revenues or expenses**.
  - Third party **performs critical functions** or stores, accesses, transmits, or performs transactions on sensitive customer information.
  - Third party markets bank products or services or provides a product or performs a service involving subprime lending or card payment transactions.
  - Third party poses risks that could significantly affect earnings or capital.

MERCADIEN

Summary of Guidance *(Cont'd)*

- The FDIC reviews a financial institution's risk management program and the overall effect of its third-party relationships as a component of its normal examination process. As noted, **the FDIC evaluates activities conducted through third-party relationships as though the activities were performed by the institution itself.**

- In that regard, it must be noted that while an institution may properly seek to mitigate the risks of third-party relationships through the use of ***indemnity agreements*** with third parties, such agreements do not insulate the institution from its ultimate responsibility to conduct banking and related activities in a safe and sound manner and in compliance with law.

MERCADIEN

Risk Assessment

- Risk assessment is fundamental to the initial decision of whether or not to enter into a third-party relationship.

- The first step in the risk assessment process should be to ensure that the proposed relationship is consistent with the institution's strategic planning and overall business strategy.

MERCADIEN

Risk Assessment *(Cont'd)*

- A risk/reward analysis should be performed for significant matters, comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or performing the function in-house.

- The analysis should be considered integral to the bank's overall strategic planning, and should thus be performed by senior management and reviewed by the board or an appropriate committee.

MERCADIEN

Potential Risks Arising From Third-Party Relationships

Numerous risks may arise from a financial institution's use of third parties. Some are associated with the **underlying activity** itself, similar to the risks faced by an institution directly conducting the activity.

MERCADIEN

Potential Risks Arising From Third-Party Relationships *(Cont'd)*

- Not all of the following risks will be applicable to every third-party relationship; however, complex or significant arrangements may have definable risks in most areas.

- The financial institution's board of directors and senior management should understand the nature of these risks in the context of the institution's current or planned use of third parties.

MERCADIEN

What Are Some of These

MERCADIEN

Strategic Risk

Arises from **adverse business decisions** or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals.

- The use of a third party to perform banking functions or to offer products or services that do not help the financial institution achieve corporate strategic goals and provide an adequate return on investment exposes the financial institution to strategic risk.

MERCADIEN

Reputational Risk

Arises from **negative public opinion**.

- Third-party relationships that result in dissatisfied customers, interactions not consistent with institution policies, inappropriate recommendations, security breaches resulting in the disclosure of customer information, and violations of law and regulation are all examples that could harm the reputation and standing of the financial institution in the community it serves.

MERCADIEN

Operational Risk

The risk of loss resulting from
inadequate or failed internal processes, people and systems or from external events.

- Third-party relationships often integrate the internal processes of other organizations with the bank's processes and can increase the overall operational complexity.

MERCADIEN

Transactional Risk

Arises from **problems with service or product delivery**.

- A third party's failure to perform as expected by customers or the financial institution due to reasons such as inadequate capacity, technological failure, human error or fraud exposes the institution to transaction risk.

- We become liable for their failings.

MERCADIEN

Credit Risk

Risk that a third party, or any other creditor necessary to the third-party relationship, is **unable to meet the terms of contractual arrangements with the financial institution or to otherwise financially perform as agreed**.

MERCADIEN

Compliance Risk

Risk arising from **violations of laws, rules, or regulations or from non-compliance with the institution's internal policies, procedures or business standards.**

- Compliance risk is exacerbated when an institution has inadequate oversight, monitoring or audit functions.

MERCADIEN

Other Risks

The types of risk introduced by an institution's decision to use a third party **cannot be fully assessed without a complete understanding of the resulting arrangement**.

- Third-party relationships may also subject the financial institution to liquidity, interest rate, price, foreign currency translation and country risks.

MERCADIEN

Life Cycle

Planning → **Risk Assessment & Due Diligence** → **Contracting** → **Monitoring & Performance** → **Termination**

How do you determine which third parties to assess?

Do third party contracts contain terms allowing you to assess and manage risks?

Are key controls at third parties in place and operating as expected?

Is third party risk managed during the handoff?

How do you manage data access?

MERCADIEN

Planning

Degree of evaluation during planning depends on whether vendor is considered critical.

- **Critical activity** - significant bank functions (i.e., payments, clearing, settlements, custody) or shared services (i.e., information technology) or other activities that:
  - Could cause a bank to face significant risk if vendor fails to meet expectations.
  - Could have significant customer impacts.
  - Require significant investment in resources to implement the third-party relationship and manage the risk.
  - Could have a major impact on bank operations if bank has to find alternate vendors or the outsourced activity has to be brought in-house.

MERCADIEN

Critical Activities

- Include significant functions, significant shared services, and other activities.

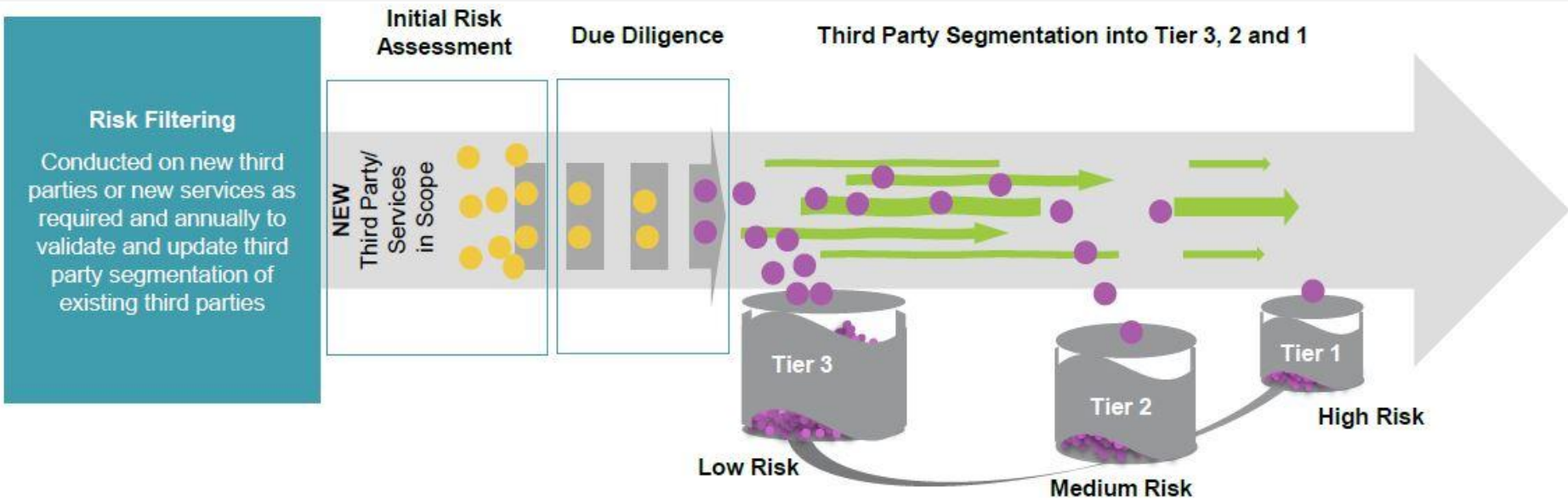
- Other critical activities may:
  - Cause a bank to face significant risk if a third party fails to meet expectations.
  - Have substantial customer impacts.
  - Require investment in resources to implement the third-party relationship and manage risk.
  - Impact operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

MERCADIEN

Risk Assessment and Due Diligence

Third Party Risk Assessment and Due Diligence

- 10 – 15 gateway questions classified into risk areas and linked to enterprise risk appetite and tolerances.
- Domain Risk Experts perform due diligence based on initial risk assessment, resulting in a residual risk-ranking score.
- Residual risk-ranking score used to segment third parties.



MERCADIEN

Due Diligence and Vendor Selection

Once potential vendors have been identified, additional due diligence should be performed before final selection.

- People (soft) skills should be considered, but not supersede potential risk of relationship.
- Risk assessment should be performed to evaluate risks and mitigating controls of relationship.
- Risk should evaluate entire relationship and activities, not just one component.

MERCADIEN

Information Security Risk

- Vendor access to Non-public Private Information (NPI).
- Vendor access to bank confidential information (i.e., strategic plans, management action plans, regulatory reports, etc.).
- Vendor access to bank premises or systems.
- Vendor provides data processing services for bank.
- Vendor provides business continuity services for bank.
- Vendor maintains customer/bank information offsite.
- Vendor has adequate physical and electronic security of their premises and systems.

MERCADIEN

Operational/Strategic Risk

- Is vendor critical to operations of the bank?
- Contract time frame and dollar value.
- Vendor due diligence procedures performed.
- Bank legal department review.
- Availability of alternative vendor for similar services.
- Compatibility of vendor products and services to the bank's strategic goals.

MERCADIEN

Relationship/Reputation Risk

- Customer interaction with vendor.
- Vendor financial strength evaluation (initial due diligence).
- Reputation of vendor.
- Vendor monitoring of its employee's activities.
- Vendor financial strength evaluation (ongoing monitoring).
- Use of other third parties by vendor.
- SSAE 16 report evaluation.
- Verification of vendor references.

MERCADIEN

Termination Steps

- Planning is key to successful termination.

- Key aspects of planning involve:
  - Understanding what happens to your data
  - Location of documents and records
  - Resolving complaints
  - Informing customers

MERCADIEN

Tips and Tricks

MERCADIEN

Vendor Management Priorities

- Vendor management allows you to build a relationship with your suppliers and service providers that will strengthen both businesses.

- Vendor management is **not** negotiating the lowest price possible. It is constantly working with vendors to come to agreements that will mutually benefit both companies.

- **Share Information and Priorities -** Provide only the necessary information at the right time that will allow a vendor to better service your needs. This may include limited forecast information, new product launches and changes in design and expansion.

MERCADIEN

Strategic Vendors

- **Balance Commitment and Competition** - gain the commitment of your vendors to assist and support your business operations.

- **Allow Key Vendors to Help You Strategize** - If a vendor supplies a key part or service to your operation, invite that vendor to strategic meetings that involve the product they work with.

  - Remember, you brought in the vendor because they could make the product or service better and/or cheaper than you.

  - They are the experts in that area and you can tap into that expertise in order to gain a competitive advantage.

MERCADIEN

Vendor Partnerships

- **Build Partnerships For The Long Term -** Vendor management seeks long-term relationships over short-term gains and marginal cost savings. Constantly changing vendors to save pennies costs more in the long run and impacts quality. Other benefits of long-term relationships include trust, preferential treatment and access to insider or expert knowledge.

- **Seek to Understand Your Vendor's Business -** Remember, your vendor is in business to make money too. If you constantly lean on them to cut costs, either quality will suffer or they will go out of business. Part of vendor management is to contribute knowledge or resources that may help your vendors better serve you. Asking questions of them will help you understand their side of the business and build a better relationship between the two of you.

MERCADIEN

Vendor Value

- **Negotiate a Win-Win Agreement -** Negotiations are completed in good faith. Look for points that can help both sides accomplish their goals. Strong-arm negotiation tactics only work for so long before one party walks away from the deal.

- **Come Together on Value -** Vendor management is more than getting the lowest price, which often brings the lowest quality. Vendor management will focus quality for the money that is paid. In other words: value! Be willing to pay more to receive better quality. If the vendor is serious about the quality they deliver, they won't have a problem specifying the quality details in the contract.

MERCADIEN

Remain Flexible

- Be wary of restrictive or exclusive relationships, e.g., limitations with other vendors or future customers. In addition, contracts that have severe penalties for seemingly small incidents should be avoided.

- If the vendor asks for an extremely long-term contract, ask for a shorter term with a renewal option.

- On the other hand, you should be open to the vendor's requests. If an issue is small and insignificant to you but the vendor insists on adding it to the contract, you may choose to bend in this situation. This shows good faith on your part and willingness to work towards a contract that is mutually beneficial to both parties.

MERCADIEN

Monitor Performance

- Don't assume that once a vendor relationship has begun that everything will go according to plan and execute exactly as specified in the contract.

- Monitor the vendor's performance constantly in the beginning, especially the requirements most critical to your business, i.e., shipping times, quality of service performed, order completion, call answer time, etc.

- Bottom line is communication, communication, communication!
  - Don't assume vendor intimately knows your business or reads minds.
  - Well-established and maintained lines of communication will avoid misunderstandings and proactively address issues before they become problems.

MERCADIEN

Contact

Raji Sathappan, MBA, CRCM, CAMS, CISA
Director, Financial Institutions Services
The Mercadien Group

rsathappan@mercadien.com
609-689-9700
Mercadien.com

MERCADIEN