rma
THE RISK MANAGEMENT ASSOCIATION

JOIN. ENGAGE. LEAD.

6 CORE ELEMENTS OF EFFECTIVE THIRD-PARTY RISK MANAGEMENT

Enterprise Risk • Credit Risk • Market Risk • Operational Risk • Regulatory Affairs • Securities Lending

Managing third party risk is a top priority for financial institutions. As regulatory expectations continue to evolve, institutions need to remain diligent in developing a program that mitigates the risks posed from outside vendors and protects its data, operations, and finances.

FRB Regulatory Guidance in SR 13-19 states that an effective third-party risk management program should include the following core elements: (Similar guidance and program requirements from the OCC can be found in the OCC Bulletin 2013-29.)

1. Risk assessments.
2. Due diligence and selection of service providers.
3. Contract provisions and considerations.
4. Incentive compensation review.
5. Business continuity and contingency plans.
6. Oversight and monitoring of service providers.

RISK ASSESSMENTS

- Consistent with the strategic direction and overall business strategy of the organization.
- Analyze the benefits and risks of outsourcing.
- Consider multiple qualified and experienced service providers.
- Update risk assessments regularly.

DUE DILIGENCE AND SELECTION OF SERVICE PROVIDERS

- Due diligence and evaluations will vary depending on the scope, complexity, and importance of the outsourcing arrangement.
- Engage technical experts and key stakeholders in the review and approval process.
- Key components of the due diligence process include a review of the service provider's:
  - Business background
  - Reputation
  - Strategy
  - Financial performance and condition
  - Operations and internal controls.

CONTRACT PROVISIONS AND CONSIDERATIONS

- The terms of service agreements should be defined in written contracts that have been reviewed by legal counsel prior to execution.

- Elements of the contract should include:
    - Scope
    - Cost and compensation
    - Right to audit
    - Monitoring of performance standards
    - Confidentiality and security of information
    - Ownership and license ○ Indemnification
    - Default and termination
    - Dispute resolution ○ Limits on liability
    - Insurance ○ Customer complaints
    - Business resumption and contingency plans
    - Foreign-based service providers
    - Subcontracting

INCENTIVE COMPENSATION REVIEW

- Ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in the contracts.
- Ensure an incentive compensation review is part of the ongoing due diligence process.

BUSINESS CONTINUITY AND CONTINGENCY PLANS

- Ensure each vendor has a documented DR/BCP plan.
- Maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted provider is unable to perform.

OVERSIGHT AND MONITORING OF SERVICE PROVIDERS

- Document a risk-based third-party program that adheres to regulatory requirements.
- Establish and monitor performance metrics for individual vendors.
- Create a governance structure for appropriate executive and board oversight.

This information was developed by Emily Nachlas, Director of Enterprise Risk Management, IBERIABANK as part of a presentation during RMA's Governance, Compliance, and Operational Risk Conference (GCOR) XIII on April 11, 2019.

ABOUT RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues.

Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, these 18,000 individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

Phone: 800-677-7621
Fax: 215-446-4101
Website: www.rmahq.org