IT Risk Management: Third Party Risk/Vendor Management

Agenda – Purpose of Presentation

- Define Third Party or Vendor Risk
- Identify Expectations for Third Party Risk Management Programs

What is Third Party Risk?

- The use of service providers to perform operational functions presents various risks to financial institutions.
- Some risks are inherent to the outsourced activity itself, whereas others are introduced with the involvement of a service provider.
- If not managed effectively, the use of service providers may expose financial institutions to risks that can result in regulatory action, financial loss, litigation, and loss of reputation.

What is Outsourcing from IT Standpoint?

- An institution contracts with an external party to provide different services which can include:
  - core processing
  - information and transaction processing and settlement activities supporting functions such as lending, deposit-taking, funds transfer, fiduciary or trading activities;
  - Internet related services;
  - security monitoring;
  - systems development and maintenance;
  - aggregation services;
  - digital certification services; and
  - call centers

Areas of Emphasis

- Types of risk exposure
- Board of Directors and senior management responsibilities
- Service provider risk management programs
- Additional risk considerations

Scope and Emphasis has Increased

- Applicability of guidance to outsourced activities beyond core bank processing and information technology-related services
- Enhanced risk management that institutions should have for better oversight and management of outsourcing risk
- Additional guidance pertaining to key aspects (attributes, governance, and operational effectiveness) of an institution's service provider risk management program

Types of Risk Exposure

- Compliance
- Concentration
- Reputational
- Country
- Operational
- Legal

Board and Senior Management Responsibilities

- Ensuring outsourced activities are conducted in a safe and sound manner and in compliance with appropriate laws and regulations
- Approving institution-wide vendor management policies that mitigate outsourcing risk
- Reporting to the board of directors on adherence to policies governing outsourcing arrangements

Service Provider Risk Management Program

- Program should be risk-focused and provide oversight and controls commensurate with the level of risk
- Program is highly dependent on criticality, complexity, and number of material business activities being outsourced

Elements of the Service Provider Risk Management Program

- Risk Assessment
- Due diligence for the selection of service providers
- Contract provisions and considerations
- Incentive compensation review
- Oversight and monitoring of service providers
- Business continuity and contingency plans

Risk Assessment

- Determine whether outsourcing the activity is consistent with the institution's strategic direction and overall business strategy
- Identify the associated risks, and conduct a cost-benefit analysis
- Determine the availability of qualified and experienced service providers to perform the service on an ongoing basis
- Conduct periodic updates of the risk assessment

Due Diligence and Selection of Service Provider

- Depends on the scope, complexity, and importance of the outsourced services
- Evaluate the service provider based on the following key due diligence components
  - Business background, reputation, and strategy
  - Financial performance and condition
  - Operations and internal controls

Contract Provisions and Considerations

- Provisions that should be included, but are not limited to, in a contract:
  - Scope of services
  - Cost and compensation
  - Right to audit
  - Confidentiality and security of information
  - Default and termination
  - Business resumption and contingency plans of the service provider
  - Subcontracting

Incentive Compensation Review

- Institutions should consider whether incentives might encourage the service provider to take imprudent risks
- Inappropriately structured incentives may result in reputational damage, increased litigation, or risk to the financial institution

Oversight and Monitoring of Service Providers

- Appropriate staff expertise
- Risk-based monitoring
- Financial condition
- Internal controls
- Escalation of oversight activities

Business Continuity and Contingency Considerations

- A financial institution's disaster recovery and business continuity plan should include critical outsourced services
- Assess the effectiveness of the service provider's disaster recovery business continuity plan and its alignment to the financial institution's plan

Other Considerations

- Suspicious Activity Report (SAR) functions
  - Complexity of outsourcing SAR-related functions due to the confidentiality of suspicious activity reporting
- Foreign-based service providers
  - Need to be in compliance with applicable U.S. laws, regulations, and regulatory guidance
  - Need to be considered with regard to foreign-based laws and regulations concerning the financial institution's ability to audit the foreign-based service provider

Other Considerations

- Internal audit
- Sarbanes-Oxley Act of 2002
  - Prohibits a registered public accounting firm from performing internal audit services for a public company client for whom it performs financial statement audits
- Risk management activities
  - Appropriateness of service provider's model

What is the Guidance

- Consists of SR 13-19/CA 13-21 letter (Guidance on Managing Outsourcing Risk) and an attached policy statement on managing outsourcing risk
- Supplements existing guidance for technology service providers
  - Refer to the FFIEC Outsourcing Technology Services Booklet (June 2004) at http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
- Applies to all financial institutions supervised by the Federal Reserve