Guidance on Managing Outsourcing Risk

March 5, 2014

Roger Pittman
Director of Examinations
Supervision and Regulation
Federal Reserve Bank of Atlanta

Neha Contractor
Supervisory Financial Analyst
Banking Supervision and Regulation
Federal Reserve Board of Governors

Ask the Fed® is a program of the Federal Reserve for senior officials of state member banks, bank holding companies, savings and loan holding companies, and state bank commissioners. Use of the presentation materials, including audio recording of a presentation, is strictly prohibited except by written permission of the Federal Reserve Bank of St. Louis. The opinions expressed in the presentations are statements of the speaker’s opinion, are intended only for informational purposes, and are not formal opinions of, nor binding on, the Federal Reserve Bank of St. Louis, or the Board of Governors of the Federal Reserve System. Each participant is responsible for its own business, financial, investment or credit decisions.
Welcome, Everyone

• Today’s session
• Questions:
  – Email your question to: askthefed@stls.frb.org
  – Use the “Ask a Question” feature on the Ask the Fed® website: www.askthefed.org
  – Click the “Ask Question” button in the webinar tool
• This call is being recorded and will be available immediately following the session.
• A short survey will be delivered via email following the call. Please let us know your thoughts about today and ideas for future sessions.
Our Presenters and Host Today

Roger Pittman
Federal Reserve Bank of Atlanta

Neha Contractor
Federal Reserve Board of Governors

Julie Stackhouse
Federal Reserve Bank of St. Louis
Background

- Horizontal review of mortgage activities
- Internal request for broadening the application of existing interagency guidance
What is the Guidance?

• Consists of SR 13-19/CA 13-21, “Guidance on Managing Outsourcing Risk,” and an attached policy statement on managing outsourcing risk

• Supplements existing guidance for technology service providers

• Applies to all financial institutions supervised by the Federal Reserve
What’s New?

• 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
Areas of Emphasis

- Types of risk exposure
- Board of directors and senior management responsibilities
- Service provider risk management programs
- Additional risk considerations
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 to the risk assessment.
Due Diligence and Selection of Service Providers

• 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

- Examples of provisions that should be included in a contract (not an exhaustive list):
  - 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 risks 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.
Additional Risk Considerations

• Suspicious Activity Report (SAR)
  – Complexity of outsourcing SAR-related functions due to the confidentiality of suspicious activity reporting

• Foreign-based service providers
  – Need for compliance with applicable U.S. laws, regulations, and regulatory guidance
  – Need for consideration with regard to foreign-based laws and regulations concerning the financial institution’s ability to audit the foreign-based service provider
Additional Risk Considerations (continued)

• 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
To Ask a Question

- Email your question to: askthefed@stls.frb.org
- Use the “Ask a Question” feature on the Ask the Fed® website: www.askthefed.org
- Click the “Ask Question” button in the webinar tool
Thanks for joining us.

www.askthefed.org