Guidance for Managing Third-Party Risk

Chicago Region
Regulatory Conference Call
December 8, 2010

Introduction

- Teresa Sabanty, Assistant Regional Director, Compliance
- FIL-44-2008, Guidance for Managing Third-Party Risk
- PowerPoint
- E-mail: chiconferencecall@fdic.gov
- Presenters – Senior Compliance Examiners:
  - Ruben Baez
  - Christopher Lombardo

Agenda

- Background.
- Potential Risks Arising from Third-Party Relationships.
- Risk Management Process.
- FDIC Supervision of Third-Party Relationships.
- Questions.
- Closing Remarks.

Background

- Third-Party Relationships Defined.
- Third-Party Uses.
- Third-Party Risk Management Process.

Potential Risks Arising From Third-Party Relationships

- Strategic.
- Reputation.
- Operational.
- Transaction.
- Credit.
- Compliance.
- Other.

Managing Third-Party Risks

Four Elements of Managing Risk

- Risk Assessment.
- Due Diligence.
- Contract Structuring.
- Oversight.

Risk Assessment

- Strategic Fit.
- Cost/Benefit:
  - Dollars and Risk/Reward.
  - Management Capability.
  - Long-Term vs. Short-Term.

Due Diligence

Third-Party Evaluation Criteria:

- Financial Condition.
- Experience.
- Business Reputation.
- Strategies and Goals.
- Complaints, Regulatory Actions, or Litigation.
- Ability to perform using current systems.

Due Diligence

Third-Party Evaluation Criteria (continued):

- Use of Subcontractors.
- Scope of Controls, Privacy Protections, and Audit Coverage.
- Business Continuity Plans.
- Knowledge of Consumer Protection Laws and Regulations.
- Management Information Systems.
- Insurance Coverage.

Contract Structuring & Review

- Scope.
- Cost/Compensation.
- Performance Standards.
- Reports.
- Audit.
- Confidentiality & Security.

Contract Structuring & Review

- Customer Complaints.
- Business Resumption & Contingency Plans.
- Default & Termination.
- Ownership and License.
- Indemnification.
- Limits on Liability.

Oversight

- Board and Management are Responsible.
- Monitoring.
- Reporting to the Board.

Oversight - Monitoring

- Evaluation of overall effectiveness of the program or arrangement.
- Continuing consistency with the bank's strategic goals.
- Compliance with laws and regulations.
- Review of testing interactions with customers.
- Review of complaint resolutions.
- Review of audits and corrective action.
- Licensing or registrations.
- Financial condition.
- Changes, including key individuals.
- Meeting to discuss performance or operational issues.

Bank Service Company Act

- FDIC FIL 49-1999
- Primary Federal Regulator Notification
- Third Party Relationships Involving:
  - Check or deposit item processing.
  - Core processing.
  - Preparation and mailing of checks, statements, or notices.
  - Any other clerical, bookkeeping, accounting, statistical, or similar functions.

FDIC Supervision of Banks' Third-Party Relationships

- Board and Management Responsibility.
- Examination Procedures.
- Report of Examination Treatment.
- Corrective Actions.

Questions & Answers

References

- **FIL-44-2008 Guidance for Managing Third-Party Risk**
- **FIL-105-2007 Revised IT Officer's Questionnaire**
- **FIL-52-2006 Foreign-Based Third-Party Service Providers**
- **FIL-27-2005 Guidance on Response Programs**
- **FIL-121-2004 Computer Software Due Diligence**
- **FIL-23-2002 Country Risk Management**
- **FIL-68-2001 501(b) Examination Guidance**
- **FIL-50-2001 Bank Technology Bulletin: Technology Outsourcing Information Documents**
- **FIL-22-2001 Security Standards for Customer Information**
- **FIL-81-2000 Risk Management of Technology Outsourcing**
- **FIL-49-1999 Bank Service Company Act**
- **FFIEC IT Handbooks**
  - *Outsourcing Technology Services*
  - *Supervision of Technology Service Providers*
- **www.fdic.gov**

Contacts

For any questions related to the material presented in this Regulatory Conference Call, you may contact via email:

Ruben Baez

or

Christopher Lombardo

at

chiconferencecall@FDIC.gov