Vendor Management

Outsourcing Technology Services
Objectives
Vendor Management – Outsourcing Technology Services

- Board and Senior Management Responsibilities
- Risk Management Program
  - Risk Assessment
  - Service Provider Selection
  - Contracts
  - Ongoing Monitoring
- Business Continuity Planning and Testing
- Other Available Resources
The Board can outsource a service, but cannot outsource the responsibility.

- Develop and implement risk-based policies and procedures to govern the outsourcing process
Board Responsibilities

- Develop and approve policies that establish an effective vendor management program framework
- Select a service provider that best meets the needs of the bank
- Negotiate a contract that protects the interests of the bank
- Oversee management’s implementation of the program through regular board reporting
Board and Senior Management Responsibilities
Vendor Management – Outsourcing Technology Services

- Audits
- Business Continuity Plans and Testing
- Service Level Agreements
- Information Security
- Financial Statements
- Higher-risk Service Providers
- Regulatory IT Examination Reports
Management Responsibilities

- Evaluate prospective providers based on the type of services outsourced and how critical the function is to the bank.
- Ensure each outsourced relationship supports business requirements and strategic plans, and is appropriate for the size and complexity of the bank.
- Confirm the bank has sufficient expertise to oversee and manage the relationship.
- Implement ongoing monitoring programs that prioritize activities based on the degree of risk and criticality of the services.
Risk Management Overview
Vendor Management – Outsourcing Technology Services

- Inform senior management and the board of the risks associated with outsourcing
- Ensure that outsourcing arrangements are prudent and consistent with business objectives
- Implement effective controls to address identified risks
- Perform ongoing risk monitoring to identify and evaluate changes in risk from the initial assessment
- Document procedures, roles, responsibilities, and reporting mechanisms
Risk Management Overview
Vendor Management – Outsourcing Technology Services

- Monitoring
- Risk Assessment
- Vendor Management
- Contracts
- Selection

FEDERAL DEPOSIT INSURANCE CORPORATION
Risk Management Overview
Vendor Management – Outsourcing Technology Services

- Monitoring
- Risk Assessment
- Vendor Management
- Contracts
- Selection
Risk Management Overview
Vendor Management – Outsourcing Technology Services

Monitoring → Risk Assessment

Vendor Management

Contracts → Selection
Risk Management Overview
Vendor Management – Outsourcing Technology Services

- Monitoring
- Risk Assessment
- Vendor Management
- Contracts
- Selection
Risk Management Overview
Vendor Management – Outsourcing Technology Services

Risk Assessment
Vendor Management
Contracts
Selection
Monitoring
Risk Assessment
Vendor Management – Outsourcing Technology Services

**Risks**

**Strategic**
- Planning, implementation, scalability

**Compliance**
- Legal and regulatory requirements

**Reputational**
- Errors, delays, omissions, fraud, breaches

**Interest Rate**
- Errors, inaccurate assumptions

**Liquidity**
- Service disruptions, settlement delays

**Cyber**
- Disruption, malware
Risk Assessment
Vendor Management – Outsourcing Technology Services

Quantifying Risks

- Outsourced Function
  - Criticality
  - Data sensitivity
  - Transaction volume

- Service Provider
  - Financial strength
  - Industry experience
  - Location

- Technology
  - Reliability
  - Security
  - Scalability
Vendor Selection
Vendor Management – Outsourcing Technology Services

- Monitoring
- Risk Assessment
- Vendor Management
- Contracts
- Selection
Vendor Selection
Vendor Management – Outsourcing Technology Services

Due Diligence: Key Considerations

- Corporate history, qualifications, references
- Financial condition
- Service delivery capability
- Technology and system architecture
- Internal control environment, security history, audit coverage
- Reliance on and success in managing subcontractors
- Legal and regulatory compliance
- Insurance coverage
- Site visits
- Disaster recovery/business continuity
Contracts
Vendor Management – Outsourcing Technology Services

Monitoring → Risk Assessment

Vendor Management → Selection

Contracts
Contracts
Vendor Management – Outsourcing Technology Services

Common Provisions

Scope of Service
• Rights and Responsibilities
  • Description of Activities
  • Timeframes for Implementation
  • Assignment of Responsibilities

Security and Confidentiality
• Responsibility and Controls
• Incident Response and Notification Requirements
• Appendix B to Part 364 (GLBA)
Contracts
Vendor Management – Outsourcing Technology Services

Common Provisions

Internal Controls
- Records Maintenance
- System Monitoring
- Notification Requirements
- Cybersecurity

Audit
- Types of Audits
  - Financial
  - General Controls
  - Network Security Assessments
  - Electronic Funds Transfer
  - Disaster Recovery Tests
- Frequency
- Right to Receive
- Right to Audit
Contracts
Vendor Management – Outsourcing Technology Services

Common Provisions

Reports
- Frequency and Types
  - Performance
  - Financials
  - Compliance with regulatory guidance

Business Resumption/Contingency Plans
- Backup and Records Protections
  - Equipment
  - Programs and Data Files
- Maintenance and Testing
  - Frequency
  - Availability of Test Results
  - Bank Participation
Contracts
Vendor Management – Outsourcing Technology Services

Common Provisions

Sub-contracting
- Awareness
- Assessment
- Responsibility

Regulatory Compliance
- Adherence to Regulatory Guidance
  - Risk Management
  - Consumer Compliance

Performance Standards
- Measurable
- Minimum Service Level Requirements
- Remedies
- Service Level Agreements (SLAs)
Banks should notify their primary Federal regulator of the outsourcing relationship within:

- 30 days of entering into the contract, or
- performance of the services

……..whichever occurs first

Bank Service Company Act Notification
## Contracts

**Vendor Management – Outsourcing Technology Services**

### SLAs

<table>
<thead>
<tr>
<th>Service</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality of Data</td>
<td>GLBA compliance, notifications, responsiveness</td>
</tr>
<tr>
<td>Integrity and Availability</td>
<td>Error rates, up time, processing timeliness</td>
</tr>
<tr>
<td>System Changes</td>
<td>Programming changes, system updates</td>
</tr>
<tr>
<td>Security Standards</td>
<td>Compliance, independent testing</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Backup, retention, protection, restoration, recovery</td>
</tr>
<tr>
<td>Help Desk Support</td>
<td>Responsiveness, availability, qualifications</td>
</tr>
</tbody>
</table>
Monitoring
Vendor Management – Outsourcing Technology Services

- Monitoring
- Risk Assessment
- Vendor Management
- Contracts
- Selection
Monitoring
Vendor Management – Outsourcing Technology Services

- Periodically reevaluate active service providers
- Tailor ongoing monitoring using a risk-based approach considering:
  - Criticality of the services
  - Sensitivity of data
  - Degree of perceived risk
- Implement more frequent and stringent ongoing monitoring for higher-risk service providers
- Report results to the board
Monitorin
g
Vendor Management – Outsourcing Technology Services

- Audit reports
  - Performed by qualified and independent personnel
  - Type, scope, and frequency consistent with:
    - Size and complexity
    - Products and services
    - Level of risk
  - Review corrective actions
Financial Condition

- Continuity of operations
- Support for the contracted services
- Investment in security controls
- Product updates
Monitoring
Vendor Management – Outsourcing Technology Services

- Compliance with Service Level Agreements
  - Performance standards
  - Information security standards (GLBA)
  - Incident response programs

- Business Continuity Plans
Monitoring
Vendor Management – Outsourcing Technology Services

- Available only to client banks under contract
- Request from FDIC Regional Office Case Manager
- National and State-member banks may request from the bank’s primary Federal regulator
Business Continuity Planning
Vendor Management – Outsourcing Technology Services

- Monitoring
- Risk Assessment
- Vendor Management
- Contracts
- Selection

Business Continuity Planning
Review service provider plans

- Mission critical service restoration
  - Timeframes and recovery time objectives
  - Staffing, capacity, telecommunications, hardware, software, and facilities availability
  - Wide-scale disruptions
- Contingency plan testing and testing scenarios
  - Connectivity, functionality, volume, and capacity of alternate facilities
  - Annual or more frequent
- Interdependencies
  - Internal and external dependencies
  - Test where feasible
Outsourcing to Foreign Service Providers
Vendor Management – Outsourcing Technology Services

- Arrangements should be subject to the same due diligence and assessment processes as domestic outsourcing relationships
- Risks become unique
Summary: Review

- Monitoring
- Risk Assessment
- Vendor Management
- Contracts
- Selection
Summary: Review

Monitoring (left) → Risk Assessment (right)

Vendor Management (center)

Contracts (bottom left) → Selection (bottom right)
Summary: Review

1. Monitoring
2. Risk Assessment
3. Vendor Management
4. Contracts
5. Selection

---

FEDERAL DEPOSIT INSURANCE CORPORATION
Summary: Review

Monitoring → Risk Assessment

Vendor Management

Contracts → Selection
Resources
Vendor Management – Outsourcing Technology Services

- FFIEC IT Examination Handbook (www.FFIEC.gov)
FDIC Financial Institution Letters (FILs)

- FIL-44-2008: Guidance for Managing Third-Party Risk
- FIL-52-2006: Guidance on Foreign-Based Third-Party Service Providers
- FIL-121-2004: Computer Software Due Diligence
- FIL-23-2002: Country Risk
- FIL-81-2000: Risk Management of Technology Outsourcing
- FIL-49-99: Bank Service Company Act

Website: www.fdic.gov
Resources
Vendor Management – Outsourcing Technology Services

- Directors’ Resource Center
  www.fdic.gov/regulations/resources/director/

- Technical Assistance Video Program
  - Information Technology (IT)
  - Corporate Governance
  - Third-Party Risk
  - Cybersecurity Awareness
  - Cyber Challenge: A Community Bank Cyber Exercise

- Questions
  supervision@fdic.gov