Comptroller of the Currency
Administrator of National Banks

Outsourcing Technology Services
A Management Decision

A Telephone Seminar for National Banks

Tuesday, July 20, 2004

And again on

Wednesday, July 21, 2004

Agenda

- Outsourcing activities and relationships
- Regulatory guidance and expectations
- Risk management process
- Examiner focus
- Hot topics
  - Foreign outsourcing considerations
  - Intrusion and Incident Response
- Recap
- Question and Answer Session

Commonly Outsourced Technology Services

- Core bank processing
- Disaster recovery
- Wholesale payments
- ACH processing
- Credit card network/switching
- Customer service/call centers

Commonly Outsourced Technology Services (continued)

- Aggregation
- Web site hosting
- Imaging and electronic safekeeping
- Network management
- Security monitoring
- Digital certificate services

Types of Technology Service Providers

- Financial institutions
- Non-banks
- Independent data centers
- Joint ventures
- Limited liability corporations
- Bank service corporations

Outsourcing and Third-Party Guidance

FFIEC IT Handbook	Outsourcing Technology Services Booklet
OCC Bulletin 2001-47	Risk Management Principles for Third-Party Relationships
OCC Bulletin 2002-16	Bank Use of Foreign-Based Third-Party Service Providers
Advisory Letter 2001-8	Standards for Safeguarding Customer Information

Outsourcing and Third-Party Guidance

FFIEC IT Handbook	Supervision of Technology Service Providers Booklet
OCC Bulletin 2004-20	Risk Management of New, Expanded, or Modified Bank Products and Services
Advisory Letter 2000-12	Interagency Guidance on IT Outsourcing
OCC Bulletin 98-38	PC Banking
OCC Bulletin 98-3	Technology Risk Management

Risk Management Process

1. Risk assessment
2. Due diligence
3. Written contracts
4. Ongoing monitoring

Risk Assessment

- Identify outsourcing risks
- Assess internal expertise
- Identify infrastructure
- Measure cost/benefit relationship
- Assess impact on Information Security Program
  - ***GLBA Section 501(b)***

Risk Assessment – Common Problems

- Failing to recognize and mitigate the risks
- Underestimating the risks involved
- Failing to devote the appropriate resources **prior** to implementation
- Allowing economic pressure to limit spending on needed controls

The risk assessment is the foundation upon which you develop and maintain your risk management process.

Due Diligence

Is this a company you want to do business with?

- Check references
  - Peers
  - User Groups
  - Better Business Bureau
  - Law enforcement
- Determine expertise
- Assess reliability
- Understand vendor management practices
  - Subcontractors

Due Diligence

- Determine adequacy of risk management process
- Assess effectiveness of controls
- Determine servicer's capability
- Analyze servicer's financial condition

Contracts

Issues banks should consider addressing in contracts:

- Scope of arrangement
- Description of fees and costs, including purchasing and maintaining hardware and software
- Service Level Agreements (SLA)
- MIS
- Audit requirements and reports
- Business resumption and contingency planning
- Regulatory requirements clause
- Data ownership and use

Contracts

Issues banks should consider addressing in contracts- continued:

- Security and confidentiality
- Intrusion and data compromise alerts
- Indemnification
- Insurance coverage
- Dispute resolution
- Default and termination
- Customer complaints
- Services subject to OCC examination and oversight

Contracts

Key provisions in contracts:

- Data ownership
  - Data may be servicer's largest asset in bankruptcy
  - May not have access to it if not specified
- Service level agreements:
  - Response time
  - System availability
  - Data integrity benchmarks
  - Economic incentives and penalties
  - Report availability and timing

Contracts

Key provisions in contracts - continued:

- Responsibilities in key areas should be clear
  - Customer complaints
  - Business resumption/contingency planning
  - Regulatory requirements clause
  - GLBA 501b compliance
  - Data compromise/Intrusion/Detection/ Monitoring/Incident Response

Contracts

Key provisions in contracts - continued:

- Bank access to audit reports
  - Specify right to review audit reports of servicer in a timely manner.
  - This right helps bank to meet its 501(b) monitoring obligation.

Contracts

Key provisions in contracts - continued:

- Termination and Exit Clauses
  - Include clause to allow either party to terminate under certain circumstances.
  - Contain detail on termination fees and the responsibilities of the servicer and the bank in the event of early termination, whether planned or not.
  - Termination fees should not be excessive or unreasonable.
  - Contract should permit an orderly transition to new vendor.

Ongoing Monitoring and Oversight

Financial condition of the service provider

- On-going monitoring
  - Audited financial statements
  - Servicer's ability to meet obligations
  - Adequacy of IT insurance coverage
- Activate contingency plan if condition unstable or deteriorating

Ongoing Monitoring and Oversight

General control environment of service provider

- Internal and security controls
  - Internal and external audits
  - Security and regulatory reports
- Policies addressing changes in products/services or regulatory requirements
- Business resumption contingency planning and testing
- User group issues
- Vendor management of subcontractors

Ongoing Monitoring and Oversight

Quality of service and support

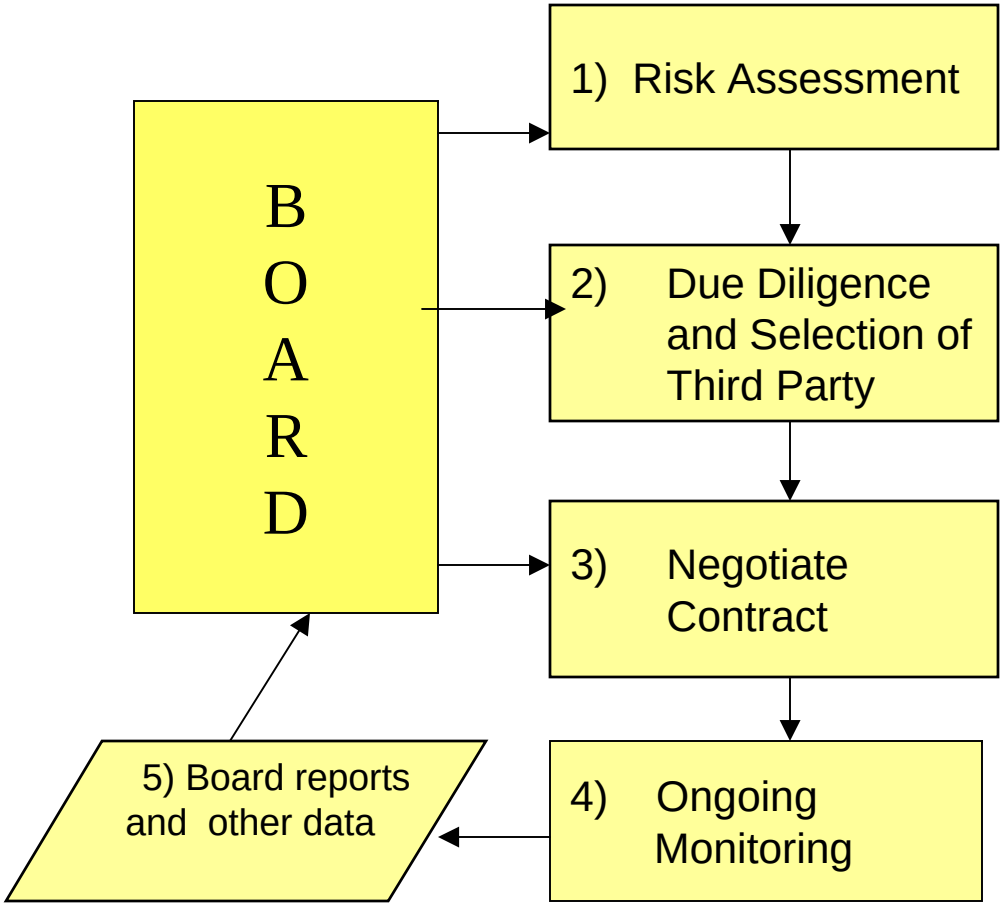
- Performance relative to contract and SLA's
- Customer complaints
- Training provided to employees
- Regular meetings with servicer to discuss performance

On-going Monitoring and Oversight

Report to the Board of Directors

- Recap of significant service providers
- Policy compliance
- Business plans for new products and services
- Risk management and performance reports
- Periodic updates - annually or more frequent as needed

Dynamic Risk Management Process



The Board should be involved in the entire process.

Examiner Focus

In assessing your risk management process, examiners may review:

- Business plans for significant, newly outsourced functions
- Risk assessments
- Due diligence reviews
- Contracts
- MIS from third party
- Ongoing monitoring and documentation
- Board reporting

Hot Topics

Foreign Outsourcing

Intrusion and Incident Response

Foreign Outsourcing - Regulatory Guidance

- OCC Bulletin 2002-16 Bank Use of Foreign-Based Third Party Service Providers

- Appendix C of the FFIEC IT Handbook, Outsourcing Technology Services Booklet

Foreign Outsourcing - Additional Risks

Country Risk

- Economic, social, and political conditions
- Impact on servicer's ability to perform contractual obligations

Compliance Risk

- Impact on bank's compliance with US and foreign laws
- OFAC's sanctions and embargo provisions
- Requirements on exportation of encryption-related technologies
- Ability to enforce contracts
- Jurisdictional considerations

Foreign Outsourcing - Additional Risks

Operational Risk

- Accessibility and ownership of bank data
- Ability to monitor/control overseas operations

Foreign Outsourcing - Contracts

Specific contracts provisions

- Choice of law and choice of forum
- Privacy and security obligations
- Continued bank ownership of data
- OCC's authority to examine foreign servicer

Foreign Outsourcing – Ongoing Monitoring

Monitoring and oversight complexities

- Reliable financial data
- Performance and quality data
- Geographic and time zone considerations

Foreign Outsourcing – OCC Examinations

OCC Focus

- Assess the bank's risk management process
- Require English translations of critical documents
- Examination of services performed by foreign-based servicer

Intrusion and Incident Response

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

- Proposed guidance issued for comment August 2003; final version will be issued soon.
- Binding interpretation of GLBA 501(b) GLBA and Guidelines.
- Requires banks to implement a response program after unauthorized access to customer information.
- Applies to information held by service providers.

Intrusion and Incident Response

Response Program requirements:

- Assess the situation
- Notify regulators & law enforcement (SAR)
- Initiate containment and control measures
- Implement corrective measures
  - Flag accounts; secure accounts
  - Provide customer notice

Intrusion and Incident Response

Proposed Guidance - Contracts

- OCC Bulletin 2001-47: service contracts should require client bank notification of security breaches at the servicer resulting in unauthorized access to customer information.
- Proposed guidance would mandate such notification provisions in servicer contracts.

Outsourcing Recap

- Outsourcing **IS** a management decision.
- Arrangement can be a safe way to improve earnings.
- The Board has ultimate responsibility.
- Risk management process should be commensurate with the risks.

Outsourcing Recap

- Outsourcing is subject to the same risk management process as if it were performed internally.
- Outsourcing to affiliates should be structured similarly as outsourcing to non-affiliates.
- Outsourcing to foreign servicers based on same principles as those for domestic companies.
- Have an adequate response program and customer notification process within your Information Security Program.

Follow-up questions and OCC website

Contact your Portfolio Manager, Assistant Deputy Comptroller, or Large Bank Examiner-in-Charge regarding any technology outsourcing question you might have.

The OCC website, www.occ.treas.gov has links to all guidance documents mentioned in this presentation.

Question and Answer Segment