Supervision of IT Risks

Information Technology Risks

Heidi Richards
Federal Reserve Board
Overview

• Internet Banking: What’s Different?
• Information Technology Risks
  – Financial
  – Operational
  – Compliance
• Supervisory Approaches
Internet Banking Risks

- Two Distinct Models:
  
  I. Established banks providing services over the Internet
  
  II. Internet banks
Internet Banking

• Established banks
  - Vast majority of Internet banking activity
  - Internet typically a small percentage of total retail customers
  - Corporate customers
  - “Trade name” banks (Wingspan)
Internet Banking Risks

- Internet-Only Banks in the United States
  - E*Trade Bank
  - NetBank
  - CompuBank
  - First Internet Bank
- Less than 20 in United States
Internet Banking Risks

• Internet-Only Banks
  - Licensing regime is not different
  - Reporting regime is not different
  - Supervisory expectations are not different
    • Management expertise
    • Business plan
    • Capital
    • Compliance
Internet Banking Risks

• Internet-Only Banks
  - Unique business model
    • High marketing/advertising costs
    • Slim interest margins
    • Low fees
  - Key risks are not operational
    • Profitability has been elusive
Supervision of IT Risks

Supervisory Risks

- Credit Risk
- Market Risk
- Liquidity Risk
- Operational Risk
- Legal Risk
- Reputational Risk
Supervision of IT Risks

Technology Risks

- Financial
- Operational
- Compliance
Different Classes of IT Risk

- **Small banks**
  - Purchase tested technology or outsource
  - Off the shelf from traditional vendors

- **Large Banks**
  - Develop technology
  - Partner with vendors
    - Often not traditional financial vendors
    - Controls over relationships
Technology Risks: Financial

• Impact of technology investments on earnings and capital
  - Can investments create a direct drag on earnings?
  - Costs to move processing in-house
  - Costs to resolve integration problems
  - Investments in failed ventures or unsuccessful product/services
Technology Risks: Financial

- Impact of technology activities on credit/market/liquidity risk
  - Above market rates on Internet deposits
  - Rate-sensitive deposits
  - Change in loan demographics
  - Lending/investment methodology
  - Rapid growth
Supervision of IT Risks

Technology Risks: Operational

- Security
- Availability
- Integrity
Supervision of IT Risks

Internet Banking Risks

- Rerouted transactions
- Theft of Information
- Fraud
- Hacking
- Spoofing
- Unauthorized Access
- Web-jacking
- Denial of Service
- Viruses
- Slow Access to Web Site
- Theft of Information
- Fraud
- Hacking
- Spoofing
- Unauthorized Access
- Web-jacking
- Denial of Service
- Viruses
- Slow Access to Web Site

Federal Reserve
14
Supervision of IT Risks

Internet Security

A Secure Computer
Supervision of IT Risks

Information-Only Site

No connectivity from Internet-site to the internal network
Requires a path from the Internet-site to the internal network
Supervision of IT Risks

Information Exchange Site

On-line Applications

Firewall Complex

DMZ

Internal Network

E-mail Server

Business Application Server

Figure 2
Supervision of IT Risks

Transactional Internet-Banking

Figure 3
Hacking

Breaches of web sites or internal systems, either to expose security weaknesses in software or hardware, cause damage, or theft of information or assets.
Hacking --> Impact to Bank

- Examples
- Causes
- Damage to reputation
- Cost
- Down time
- Statistics
Hacking --> Impact to Bank

- Examples
- Causes
- Damage to reputation
- Cost
- Down time
  - Dependent on contract with vendor
  - Dependent on when bank learns of hack
  - Statistics
Supervision of IT Risks

Hacking

Event

Causes

Direct Effect

IT/Operational Risk

Business Risk

Regulatory Impact

--> Impact to Bank

Web site is defaced

Weak internal controls

Customer confidence

Integrity

Reputational

CAMELS deteriorates?

Federal Reserve
Viruses

- A program that can “infect” other programs by modifying them to include a, possibly evolved, copy of itself.

- Types of Viruses:
  - Worm: a virus that replicates itself from machine to machine across networks/Internet connections often clogging networks and destroying data.
  - Others - Rabbits, Trojan horses, & etc.
Viruses --> Impact to Bank

• Examples
  - LoveBug Virus
  - Melissa Virus

• Damage to reputation
• Cost
• Down time
• Statistics
Viruses

• Examples

• Damage to reputation
  - Bank can be innocent bystander
  - Bank’s server can be used as “slave” or “zombie”

• Cost

• Down time

• Statistics

--> Impact to Bank
Supervision of IT Risks

Viruses

- Examples
- Damage to reputation
- Cost
  - Clean-up
  - Legal expense
- Down time
- Statistics

--> Impact to Bank

Melissa cost between $93 million and $385 million

LoveBug $5 to $10 billion
Viruses

• Examples
• Damage to reputation
• Cost
• Down time
  - If not caught in time can require re-formatting and re-installing all applications and data
• Statistics

--> Impact to Bank
Supervision of IT Risks

Viruses

Event

Causes

Direct Effect

IT/Operational Risk

Business Risk

Regulatory Impact

--> Impact to Bank

Bank Site Used as “slave”

Weak internal controls

Legal liability

Security

Liquidity/Legal

CAMELS deteriorates?
Unauthorized Access --> Impact to Bank

Event:
- Fraudulent transaction
- Weak internal controls
- Transaction loss
- Security
- Operational/ Reputational
- CAMELS deteriorates?

Causes:
- IT/Operational Risk
- Business Risk
- Regulatory Impact

Supervision of IT Risks
Major risks have been related to systems integration
- Integrity of information
- Availability of systems to customers

Examples:
- Wells Fargo/First Interstate merger
- Fleet/BankBoston merger
Compliance Risks

• Consumer protection rules
  - Unique to each country
  - Often involve disclosure requirements
  - Electronic environment may pose challenges
  - United States: ESign Act
Supervisory Approaches

• IT Audit
• IT Examinations/Ratings
• Business Line/MIS Approach
• Operational Risk
IT Audit Approach

- IT Auditors
  - Input $\Rightarrow$ Processing $\Rightarrow$ Outputs

- IT auditors test transactions to ensure input properly translated into outputs
  - System Development Life Cycle
IT Examinations

• U.S. banking agencies historically conducted separate IT examinations
  - 2-3 year frequency
  - Separate presentation of findings
• Federal Reserve recently eliminated separate exams
  - All examinations now to include risk-focused IT component
  - Integrated report
Supervisory Approaches: Traditional IT Review Methodology

- Audit Coverage
- Management
- Systems & Programming
- Quality Assurance
- Operations
- Information Security
- Contingency
- Telecommunications
- Outsourcing
IT Rating System

- Used by all federal banking regulators in United States for banks with material in-house processing
- Based on COBIT IT Audit model
- 4 components and composite rated on 1 to 5 scale
Supervision of IT Risks

IT Rating System

- Audit
- Management
- Development & Acquisition
- Support & Delivery
Supervision of IT Risks

IT Rating: Audit

• Independence
• Adequacy of Risk Analysis
• Scope, Frequency, Accuracy, Timeliness of Reports
• Audit participation in Application Development, Acquisition and Testing
• Auditor Qualifications
Supervision of IT Risks

IT Rating: Management

- Director Oversight and Support
- Management Depth and Succession
- Adequate Strategic Planning
- Responsiveness to Changing Business Conditions
- IT Plans, Policies, Procedures, and Standards
- Performance Reporting, e.g. Operations, MIS
Supervision of IT Risks

IT Rating: Development and Acquisition

- Systems Development, Acquisition and Change Management
- Identification and Implementation of IT Solutions
- Project Management
- Testing
- Program change controls
Supervision of IT Risks

IT Rating: Support and Delivery

• Security Administration
  • Formal Policy and Awareness Program Communicated and Enforced Enterprise-wide
  • Logical and Physical Security Closely Monitored, With Incidents Communicated and Resolved

• Continuity Planning
  • Comprehensive DRP and BRP
  • Provisions Current and Tested
  • Pre-defined Recovery Time Frames
Supervision of IT Risks

IT Rating: Support and Delivery

• Operations Management
  - Service Level Performance
  - Adherence to Defined SLA’s

• Monitoring of Third Party Relationships
Support and Delivery: Outsourcing

- Transfer of Direct Managerial Responsibility
- Include Use of Affiliates
- Activities Include Information Technology, Audit, Loan Review, EFT
- Reduced Costs
- Access to Expertise
Supervision of IT Risks

Outsourcing Arrangements

- Third-party Service Provider
- Affiliated Service Provider
- Facilities Management
- Turnkey Application
- Service Bureau
- Independent Data Center
Supervision of IT Risks

Outsourcing Vendors

• Core Bank Processing
  - FiServ
  - EDS
  - Alltel
  - Jack Henry & Associates

• Internet Banking
  - S1
  - Digital Insight
  - Corillian
  - Netzee
Outsourcing Risk Management

- Risk Assessment
- Selection of Service Provider
- Contracts
- Controls
- Ongoing Monitoring
- Information Access
- Audit
Supervision of IT Risks

Outsourcing Risk Management

• Reliability of Service
• Third Party Vendor’s Access to Confidential Information
• Adequacy of Vendor’s Audit Program
• Extent Vendor Uses Sub-contractors or Other Third-parties to Perform Services
Most Common IT Examination Findings

- Inadequate/No IT Audit Program
- Poor Systems Integration Management
- No Testing of Disaster Recovery Plan
- Monitoring of Outsourced Vendor
- Inadequate Security (e.g. password control)
Most Common Internet Banking Examination Findings

- Policies and Procedures not Updated
- No Board Approval, Strategic Plan, or Impact Assessment of Internet Banking
- Internet Banking not included in Contingency Plan
- No Monitoring of Outsourced Vendor
- No Audit Coverage of Internet Banking
Supervisory Approaches

Separate IT examinations
  - Increased specialist attention to technology risks
  - Risk: divergence of IT view from safety and soundness view
    - Safety and soundness examiners generally do not understand IT
    - IT examiners generally do not understand business risks
Supervisory Approaches

Point in time IT examination may be increasingly less relevant
- Business strategic risk drives IT actions
- Need business knowledge to identify risk
- IT examiner often not equipped to address
- Separate IT rating may not always be incorporated in overall risk assessment
Supervisory Approaches

New IT models are very different
- Centralized “standards” with local business ownership of IT resources
- Decentralized business ownership with some centralized support services
- Business ownership with outsourced infrastructure
- Internet Banking requires integrated approach
Supervisory Approaches: Business Line Approach

IT business model has changed
- IT rarely centralized in large organizations
- Business owns IT
- Who does the IT examiner talk to?
- How does supervisor judge IT risks in businesses without assessing the business?
Supervision of IT Risks

Business Line Approach

- Identify key business lines that rely heavily on automated systems
- Review integrity of MIS, including risk management, in conjunction with business line review
- Availability of systems that support real-time functions
Supervisory Approaches: Operational Risk

- **What is Operational Risk?**
  - Early definition - “Everything other than market and credit risk”
  - Direct or indirect losses
  - Loss events may be traced back to weaknesses in processes or people

- **Information Technology** is one component

- **Industry sound practices** beginning to emerge
Operational Risk

- Rapid Change and Consolidation
- Enterprise-Wide Risk Management
- Realization that Operational Risk is on par with Traditional Banking Risks
- Basel Committee Study on Capital Requirements
Operational Risk: Examples

- Settlement snafus
- Back-office mistakes
- Audit oversights
- Risk control lapses
- Other failures associated with the daily running of different business lines
Questions for Supervisors

- How do IT risks impact the organization’s key business functions?
- What specific IT issues need special attention at this institution because of the risks they pose?
Questions for Supervisors

- How has/is the institution handling change in its IT activities and operations?
  - New activities: Internet banking
  - Which (if any) merit supervisory review?
- Has the bank implemented IT audit and controls appropriate for its level of complexity?
Questions for Supervisors

- Are you comfortable with core aspects of the institution’s operations:
  - Reliability of service provider
  - Reliability of risk management and reporting systems
  - Security of data
  - Integrity of systems through mergers, etc.
Supervision of IT Risks

Information Resources

• US Banking Agencies web sites
• Consulting firms
• Industry IT audit associations
  - ITaudit.org
  - ISACA
Supervision of IT Risks

Questions?