BITS/American Banker Financial Services Outsourcing Conference

FFIEC Regulatory Update

Ralph Sharpe

Deputy Comptroller for Bank Technology

Office of the Comptroller of the Currency

November 15, 2002

Disclaimer

The views and opinions expressed in this presentation do not necessarily represent the views and directives of the Federal Financial Institutions Examination Council or its members.

Presentation Overview

- FFIEC IT Subcommittee Activities
  - Interagency Guidance
- Technology Trends and Risks
- IT Handbook Update
- FBIIC
- Looking Forward
- Questions?

FFIEC IT Subcommittee Activities

FFIEC IT Subcommittee

- Members include representatives from FRB, OCC, FDIC, OTS and NCUA
- IT Subcommittee reports to FFIEC Task Force on Supervision
- Vehicle for common policies, procedures and issuances
- Agencies also issue guidance tailored for their own institutions (See Summary of Regulatory Guidance on Electronic Banking)
  - See, e.g., OCC Guidance on Bank Use of Foreign-Based Third-Party Service Providers, OCC 2002-16, 5/15/02
  - See also, recent FDIC issuance of IT Examination Procedures, FIL 118-2002. 10/902

Technology Trends and Risks

Technology Trends

- **Technology Advances**
  - Faster, cheaper, more reliable telecommunications
  - Rapid advances in speed and capacity of computer chips
  - Growth of fourth generation programming languages
  - Proliferation of technology service providers

- **Technology Challenges**
  - Competition from other industries and abroad
  - Potentially lower entry costs for non-banks that want to compete for banking services
    - Payment systems
    - Aggregation
  - Customers increasingly view banking as commodity
  - Increased reliance on third parties with potential system access and information sharing

Technology Risks

- Key Risks Include
  - Strategic
  - Reputation
  - Compliance/Legal
  - Operational/Transaction

Strategic and Reputation Risks

- Uncertain return on investment and customer acceptance (e.g., timing)
- Evolving technology, standards, and regulations
- Reliance on third party providers
- Unproven business models (e.g., Internet-only banks)
- Increased visibility
- Customer loyalty and volatility

Legal and Compliance Risks

- Customer Privacy
- Electronic disclosures
- Electronic signatures
- Money laundering, computer crime
- Permissibility of bank activities
- Cross border oversight and regulation

Operational and Transaction Risk

- Security
  - Confidentiality (Theft of Information)
  - Data Integrity (Malicious hacking or fraud)
  - Authentication (Identify theft or fraud)
- Outsourcing/Vendor Management
- Business Continuity Planning
  - Availability
  - Reliability

Outsourcing Trends and Vendor Management Risks

Outsourcing Trends

- OCC data indicates 75% of our banks rely on 3rd parties to host Internet banking
- Pace of new technology increases reliance on third parties
- Consolidation of technology companies and bank technology service providers
- Weak or negative earnings straining cash and capital levels at some IT providers
- US Banks' IT investment is slowing -- focus on improving existing technology

FFIEC Guidance: “Risk Management of Outsourced Technology” (11/28/00)

- Key elements of the risk management process:
  - Risk assessment
  - Due diligence in selecting service provider
  - Contract Requirements
  - Oversight of service provider

Regardless of the decision to outsource, the bank remains ultimately responsible.

Regulatory Oversight of Service Providers

- Authority derives from the Bank Service Company Act of 1962
- Interagency exams are coordinated by the FFIEC Information Systems Subcommittee
  - MultiRegional Data Processing Servicer Program (MDPS)
  - Shared Application Software Review Program (SASR)
- Recently, Internet banking service providers have been included in the MDPS program
- Onsite exams are staffed by examiners from all agencies and a joint report is produced

Regulatory Oversight of Service Providers

- Exam reports are not a substitute for due diligence and oversight by bank management (e.g., regular receipt of independent audits and security reviews)
- The scope and frequency of the exams should be considered when using the reports as a resource

FFIEC Information Technology Examination Handbook Update

FFIEC Information Technology Examination Handbook Update

- Ongoing Project to Update 1996 Handbook
- No Longer Only Paper Based
- Format Changed to Sections or Booklets to be issued when completed
- Risk-Based Procedures vs Checklists

FFIEC Information Technology Examination Handbook Update

- Nine sections being updated: IT Security, E-Banking, Technology Service Providers, Payment Systems (3 sub-sections), Outsourcing, Audit and Business Continuity
- Target - From Draft to Field Testing to Roll Out between now and end of 2Q03
- Infobase training will be available with each Handbook – similar to FFIEC Privacy Training

Financial and Banking Information Infrastructure Committee (FBIIC)

FBIIC - Background

- Created by Executive Order 13231, October 2001
- FBIIC is a standing committee of the President's Critical Infrastructure Protection Board, serves as the Office of Homeland Security Financial Markets Work Group.
- FBIIC is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system.
- Treasury's Assistant Secretary for Financial Institutions chairs the committee.

FBIIC Background, Cont'd

- **FBIIC Members Include:**
  - Commodity Futures Trading Commission
  - Conference of State Bank Supervisors
  - Federal Deposit Insurance Corporation
  - Federal Reserve Board
  - National Association of Insurance Commissioners
  - National Credit Union Administration
  - Office of Cyberspace Security
  - Office of the Comptroller of the Currency
  - Office of Federal Housing Enterprise Oversight
  - Office of Homeland Security
  - Office of Thrift Supervision
  - Securities & Exchange Commission

Current Focus of FBIIC Efforts

- Establishment of secure communications facilities for FBIIC agencies
- Review and update of Agency Continuation and Operations Plans (COOP)
- Evaluation of financial sector vulnerabilities
- Coordination of communication with OHS, private sector, international counterparts, other critical sectors
- Government Emergency Telecommunications Services (GETS) and Telecommunication Service Priorities (TSP) Policies
- See FBIIC Website for additional information www.fbiic.gov

Technology Risk Challenges Looking Forward

- Basel II Operational Risk Issues
  - Basle II to be finalized in 2003; fully implemented by the end of 2006
  - Adds requirement for capital standards for Operational Risk
  - Mandatory only for a small number of institutions – but others may volunteer to be included
  - Definition of Ops Risk: "The risk of loss resulting from inadequate or failed internal process, people or systems, or from external events."

Basel July 2002 Sound Practices for Management of Ops Risk

- Includes Management of:
  - Internal and external fraud
  - Employment practices and workplace safety
  - Client products and business practices
  - Damage to physical assets
  - Business disruption and systems failures
  - Execution, delivery and process management
- Note re Outsourcing
  - (See paragraphs 39-40): growing use of outsourcing can mitigate some risks but also "present significant other risks"
- Board/Management Responsibilities
  - Responsibility of Board not diminished re safety/soundness and compliance; need for rigorous legal agreements, due diligence and monitoring

IT Governance

- Purpose of IT Governance
  - "The purpose of IT governance is to direct IT endeavors, to ensure that IT's performance meets the following objectives:
    - For IT to be aligned with the enterprise and realize the promised benefits
    - For IT to enable the enterprise by exploiting opportunities and maximizing benefits
    - For IT resources to be used responsibly
    - For IT-related risks to be managed appropriately "
    - See www.itgovernance.org

Potential 501(b) Issues

- 501(b) required FIs to establish physical, technical, & administrative safeguards to protect the privacy of customers' nonpublic information
- Contract Review Issues
- Enforcement Issues
- Interface with FTC Rules

Miscellaneous Issues

- Electronic Record Retention
  - Accuracy, Integrity and accessibility
- Weblinking/Shared Electronic Space
- Wireless Networking
- Others?

For more information see Web sites of banking agencies

- FDIC: www.fdic.gov
- FRB: www.frb.gov
- OCC: www.occ.treas.gov
- OTS: www.ots.treas.gov
- NCUA: www.ncua.gov
- FFIEC: www.ffiec.gov

Questions?