Information Technology Risk

Joint World Bank/Federal Reserve System Seminar for Senior Bank Supervisors from Emerging Economies

Adrienne Haden & Mike Wallas
Board of Governors of the Federal Reserve System
November 5, 2002
Overview

- Banking Risks
  - Traditional Risk Elements
  - Technology Risk Elements
- Internal Controls
- Vendor Management/Outsourcing
- Supervision Integration
- Third Party Service Providers
- Interagency Reference Materials
Traditional Risk Elements

- Credit
- Market
- Liquidity
- Operational
- Legal
- Reputational

SR 95-51
Rating the Adequacy of Risk Management Processes and Internal Controls
Technology Risk Elements

- Management Processes
- Architecture
- Integrity
- Security
- Availability

SR 98-09
Assessment of Information Technology in the Risk-Focused Framework
Technology Risks

- Breaches of policies
- Inadequate Separation of Duties
- Unauthorized Access
- Web-jacking
- Natural Disasters
- Denial of Service
- Hacking
- Identity Theft
- Data Center Burns
- Audit oversights
- Inadequate Password Administration
- Systems Not Integrated
Risk Relationships

SR 95-51
- Credit
- Market
- Liquidity
- Operational
- Legal
- Reputational

SR 98-09
- Management Process
- Architecture
- Integrity
- Security
- Availability

Credit
- Collateral
- Interest Rate
- Foreign Exchange
- Commodities
- Funding
- Fire, floods, accidents
- Theft, Fraud
- Operations and Administration Errors
- Fiduciary
- Regulatory
- Political
- Social
Defining IT Risk

- Management Process
- Architecture
- Integrity
- Security
- Availability
Management Processes

- Management processes involve planning, investment, development, execution, and staffing of information technology functions.
- Should be consistent with the organization’s mission and business objectives.
- Strategic planning
- Management
  - reporting
  - succession
  - independent review
Architecture

- Architecture refers to the underlying design of an information system and its individual components.
- Physical and logical architecture
- Individual components
- Meets current & long term business objectives
- Address capacity requirements
- Adequate interface between systems
Integrity

• Integrity refers to reliability, accuracy, and completeness of information delivered to users.

• An effective level of integrity is measured by:
  – accuracy
  – completeness

• Insufficient integrity could adversely affect
  – day-to-day reliability,
  – processing performance,
  – input and output accuracy, and
  – ease of use of critical information.
Security

- Security refers to safety afforded in information assets and the information processing environments,
- Commensurate with the value of the assets.
- Addresses physical and logical security
- Prevents unauthorized access, modification, destruction or disclosure during creation, processing, maintenance, storage, or transmission
Availability

- Availability refers to the delivery of information to end-users, counter-parties.
- Effective when information is consistently delivered on a timely basis in support of business and decision-making processes.
- Measures of availability include:
  - Capacity of information systems
  - Appropriate business continuity planning processes
Regulatory Expectations for Business Continuity Planning

- Comprehensive - address all critical functions of the organization.
- Ensure business processes as well as information systems are considered.
- Includes critical operations supported by external service providers.
- Test all critical components (at least annually).
- Effective data back-up and off-site storage.
All Aspects of the Organization Should be Considered

- Data centers, networks, service providers, business units
- Workspace, equipment, files, manuals, supplies, forms
- Communications
  - internal/chain of command
  - external
  - critical vs. non-critical
Testing

- Current and clear test objectives
- Cover all key aspects of contingency plans and critical business functions
- Use only materials from off-site storage
- Minimum annual testing and analysis of results
- Timely resolution of test exceptions
- Test every significant change to environment
- Recovery time and point objectives defined
- Audit involvement in testing process
No Glaring Errors or Omissions

- No recovery site
- No transportation plan
- Recovery site or off-site storage in close proximity or inappropriate location
- No restoration time/capability goals and objectives
Back-up and Offsite Storage

- Data back-up
- Frequency
- Storage location
  - Safe distance from operation/data center
  - Environmental conditions should not impact both locations
  - Disruption should not impact both locations
Regulatory Guidance

- FFIEC Supervisory Policy 5
  - Corporate Business Resumption and Contingency Planning
- FFIEC IS Handbook Chapter 10
  - Business Continuity Planning Under Revision
- FFIEC URSIT Rating
Risk management practices should promote continuity of operations and availability of data.

Support and delivery rating encompasses contingency planning.
Relating Technology Risks to Traditional Risks

Banking Activities

Traditional Risk Elements  Technology Risk Elements
Internal Controls

- Policies and procedures
- Risk assessment
- Appropriate audit function
- Adequate reporting mechanisms
- Appropriate vendor management
Policies and Procedures

- Documented in writing
- Reviewed and approved by Board of Directors
- Appropriate to size and complexity of organization
- Periodically reviewed and updated
Risk Assessment

- Identification of critical business lines or functions
- Identification of risk to these business lines
- Prioritization
- Reviewed in relation to business objectives
Audit

- Appropriate to the size and complexity of the organization
- Internal/External Audit
  - Staffing
  - Qualifications
  - On-going training
Reporting

- Board of directors
- Senior management
- Business owners
- End-users
- Periodic and timely basis
Vendor Management

- Risk Assessment
- Selection of Service Provider
- Contracts
- Controls
- Ongoing Monitoring
- Information Access
- Vendor audit program
Vendor Relationship Cycle

Contingency Plan

Life Cycle

- Vendor Contract
- Vendor Selection
- Objectives
- Manage Vendor
- Monitor Vendor
- Validate Products & Services
- Plans to Disengage or
- Contract Renewal

Vendor Relationship Cycle
Why Do Banks Outsource?

“Good Reasons” for Outsourcing:

- Bank lacks scale to implement technology independently
- Lack of technical skill sets in existing staff
- Complexities of implementing technology are a barrier to entry
- Pricing structures encourage banks to use partners
Background and Benefits

- Transfer of day to day management
- Include use of affiliates
- Activities include information technology, audit, loan review, EFT
- Reduced costs
- Access to expertise
Why Do Banks Outsource?

Bad Reasons” for Outsourcing:

- Bank management desires to move operational risks to a service provider
- Bank management perceives that outsourcing eliminates risk
- Outsourcing represents an alternative to gaining technical skills
Outsourcing

• Risks
  – Result from inadequate or ineffective vendor oversight
  – Bank loses day-to-day control of the information processing function
  – Bank’s needs and desire are not the sole driving force for the vendor or service provider

• Mitigation
  – Appropriate vendor management programs
    • Due diligence
    • Contracts
    • Monitoring
    • Periodic review
  – User group membership
  – Management and Board knowledge and understanding of the vendor relationship
Supervision Integration

Sources of Risks
- Employees
- Customers
- Others
- Operations
- Lending
- Customer Service
- Internet Activities

Technology Risks
- Management
- Integrity
- Infrastructure
- Security
- Availability

Traditional Risks
- Credit
- Market
- Liquidity
- Operational
- Legal
- Reputational
Risks, Ratings and Integration

Traditional Risk Elements

IT Risk Elements
E-Banking Risks

CAMELS
Integrated Supervision

Risk-Based Approach:

- Increased emphasis on planning and on the organization’s risk management process.
- IT included in key business lines and business risks.
- Insight into a bank’s ability to meet challenges.
- Flexible transaction testing.
Interagency Examination Program:

- Multi-Regional Data Processing Service Providers (MDPS)
- Regional Service Providers
- Examination frequency based on risk-ranked business lines and vendor specific assessments
- Uniform Rating System for Information Technology (URSIT)
Summary

- Review
  - Banking Risks
    - Traditional Risk Elements
    - Technology Risk Elements
  - Internal Controls
  - Vendor Management/Outsourcing
  - Integration
  - Third Party Service Providers
- Interagency Reference Materials
- Questions