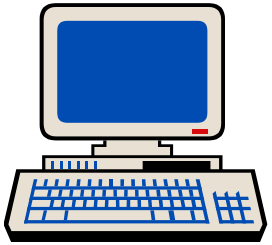
IT Risk Supervision

Outline of the Discussion



- Define IT Risk
- Identify Scope of an IT Examination
- Describe a Bank's Operating Environment
- Identify Risks Considered in IT Supervision
- Describe the IT Ratings Framework

Unique Attributes

- What is IT Risk…
  - Expansive
    - Automation and technology advancements
    - Connection to business risks
  - Dynamic
    - New risks are introduced with innovation
    - IT Strategy
  - Challenging
    - Difficult to implement policy that stays current
    - Supervision must be flexible

IT Scope - Operations

- Risk Focused IT Examinations
  - Access and Identity Management
  - Internet and Mobile Banking
  - Branch and Remote Capture
  - Wire Transfers
  - ATM Processing
  - ACH Originations
  - Virtualization / Cloud
  - Models

IT Scope – Risk Management

- Risk Focused IT Examinations
  - Information Security
  - Cybersecurity
  - Vendor Risk Management
  - Business Continuity / Disaster Recovery
  - Application Access Controls
  - Change Management
  - Data Governance
  - IT Audit Coverage

IT Scope – Environment Changes

- Risk Focused IT Examinations
  - implementation of new systems
  - significant changes in operations including mergers or system conversions
  - new or modified outsourcing relationships for critical operations
  - significant industry trends/issues
  - business lines where internal controls or risk management are heavily dependent on information technology
  - follow-up on issues raised by internal audit or in the last report of examination
  - Issues related to the use of the internet and cyber security

IT Examination Process

1. Understand Operating Environment
2. Identify Technology and Business Risks
3. Develop Risk Assessment and Conclusions
4. Rate the Institution

Understanding the Operating Environment

Outsourced	In-House	Combination
(Serviced)	(Turnkey)	(Blended)
Data processed at vendor location	Data processed at bank with purchased hardware and software	Combination of in-house and outsourced data processing
i.e. Fiserv processes items and posts transactions to the general ledger for a financial institution.	i.e. Financial institution purchases hardware and software which it uses to process items and post transactions to the general ledger.	i.e. Item processing is performed internally by bank staff and the posting of transaction of the general ledger is performed by Fiserv.

Degree of Control

- Level of IT risks - depends on degree of control
- In-house operations - 100 percent
  - retains all responsibility authority and accountability
- Outsourced operations - 0 percent
  - delegates some authority to an outside party through a contract while retaining accountability
- Vendor - 0 percent
  - products developed without bank input; carefully evaluate the risks

Identify Technology and Business Risks

Management Processes

Architecture

Integrity

Security

Availability

Management Processes

The potential that ineffective management processes result in information systems that are not adequately or appropriately aligned with the business processes and mission of the organization.

- Planning
- Investment
- Development
- Execution
- Staffing

Management Process - Key Issues

- Competitive advantage
- Critical to global competition
- Critical to a merger - whose systems to use and how to integrate
- Linkage to strategic planning
- End-users - should understand the systems and be included in decision-making

Management Process – Key Controls

Preventative:

- Strategic plan
- Succession planning
- Communications
- Staffing
- Policies/procedures
- Segregation of duties
- Cross training/job rotation
- Documentation

Detective:

- Managerial reports
- Financial reports
- Variance reports
- Employee appraisals
- Error statistics and logs
- Internal and external audit

Corrective:

- Education
- New plans or procedures
- Outsourcing
- Replacement of management

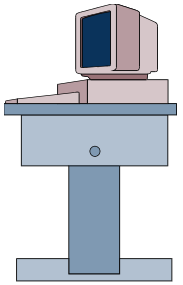
Architecture

The risk that the underlying design and individual components of an automated information system will not meet current and long-term organizational objectives.

- Compatibility
- Capacity Management
- Alignment with Business Goals

Architecture – Key Issues

- Underlying design of the information technology system and its physical and logical components:
  - Network communications
  - Hardware
  - Software: operating systems, communications software, database management systems, programming languages and desktop software



Architecture Risk - Key Controls

Preventative:

- Strategic and tactical plans
- Feasibility study
- Procurement policy
- System development methodology
- Capital plans and procedures
- Change control
- Acceptance testing

Detective:

- Inventory systems
- Self-assessment
- Internal and external audit

Corrective:

- Retrofit
- Re-engineer
- Translate/transform

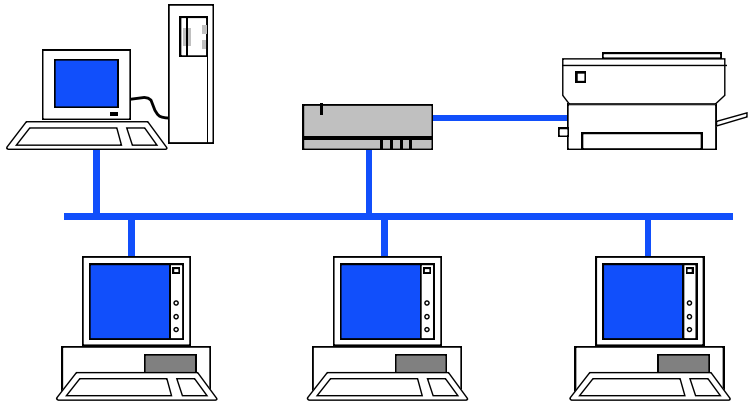
Integrity

The risk that a system, application, or computer program, and the resulting information flows, will not satisfy end-user business requirements and expectations.

- Audit Coverage
- Policies, Procedures and Practice
- Reliability, Accuracy, and Completeness

Integrity – Key Risks

- Key part of this process - System Development Life Cycle - SDLC
  - **Initiation**
  - **Requirements**
  - **Design**
  - **Programming**
  - **Testing**
  - **Implementation**
  - **Evaluation**
  - **Maintenance**



Integrity Risk - Key Controls

Preventative:

- Adherence to SDLC
- Quality assurance program
- Change control
- Acceptance testing
- Capacity planning
- Resource scheduling

Detective:

- Self-assessment
- Internal and external audit
- Acceptance testing
- Performance monitoring
- Machine diagnostics/logs
- Error statistics

Corrective:

- Redesign of application
- File rotation and retention
- Recovery and restart
- Replacement
- Reschedule demand

Security

The potential that control breaches will result in unauthorized access, modification, destruction, or disclosure of information assets during their creation, transmission, processing, maintenance, or storage.

- Information Security Program
- Physical Security
- Logical Access Management

Security – Key Risks

- Utilize preventative and detecting controls - physical and logical
- Physical - isolate mainframes and servers
- Logical - restrict access to systems and changes to systems; create audit trails; periodically review access; encrypt critical information (particularly sensitive customer information

Security Risk - Key Controls

Preventative:

- Physical/logical access control
- Capacity modeling
- Proprietary networks
- Switchability routing
- Protocols
- Public networks
- Encryption/authentication
- Access code
- Firewalls
- Vulnerability/threat assessments

Detective:

- Violation reports
- Self-assessment
- Internal and external audit
- Inventory control
- Verification/configuration
- Call back
- Batch control
- Incident response team

Corrective:

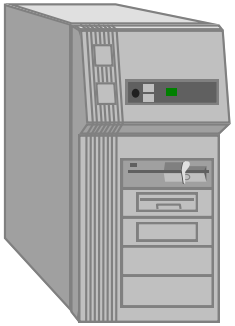
- Disaster recovery plan
- Insurance
- Retransmission/rerouting

Availability

The potential that an organization will not be able to consistently deliver information on a timely basis in support of business processes and decision making.

- Disaster Recovery Planning
- Business Continuity Procedures
- Data Backup/Recovery Process

Availability – Key Risks



- Identification of critical systems
- Data back-up sites - “hot”, “warm” or “cold”
- Regular testing of the contingency plan
- Sufficient system capacity

Availability - Key Controls

Preventative:

- Maintenance - hardware/software
- Redundancy
- Modeling
- Testing
- Diverse routing
- Physical security

Detective:

- Virus detection
- External sources
- Self-assessment
- Internal and external audit

Corrective:

- Disaster recovery plan
- Insurance
- Reciprocal agreement

Rate the Institution

- Uniform Rating System for Information Technology (URSIT)
- SR Letter 99-8
- 4 Components + Composite Rating
- Same Scale as CAMELS (1-5)

Uniform Rating System for IT

- URSIT Components
  - AUDIT
  - MANAGEMENT
  - DEVELOPMENT AND ACQUISITION
  - SUPPORT AND DELIVERY
  - COMPOSITE (1-5)

Audit Rating

- Internal Audit review includes:
  - Overall effectiveness of the audit process
  - Audit independence
  - Adequacy of risk assessment methodology
  - Scope, frequency, accuracy and timeliness of internal and external audit reports
  - Extent of audit participation in application, development, acquisition and testing
  - IT audit staff and qualifications
  - Quality and effectiveness of internal and external audit as it relates to It controls
  - Overall adequacy of plan vs. IT risks

Management Rating

- Director oversight and support
  - Adequate strategic planning
  - Review/approval of policies, contingency plan
- Senior Management
  - IT plans, policies, procedures, and standards
  - Risk management/risk identification practices
  - Vendor Management Program
  - Responsiveness to audit issues/concerns and timely corrective action
- Line Management
  - Depth and succession
  - Qualifications

Management Rating

- Management review includes:
  - Level/quality of oversight and support of IT processes
  - Effectiveness of risk monitoring systems including identification, measurement, monitoring and controlling risks
  - Management planning - new activities - succession plan
  - Adequacy of MIS reports
  - Awareness of and compliance with laws and regulations
  - Management of contracts, outsourcing, and service delivery and monitoring of the arrangements

Development and Acquisition

- Identification and implementation of IT solutions
- Project management
- IT solutions align with user needs
- Change management
- Independent quality assurance
- Testing

Development and Acquisition

- Development and acquisition review includes:
  - Oversight and support of systems development and acquisition activities by senior management and Board
  - Accountability for systems development
  - Adequacy of SDLC and programming standards
  - Quality of project management programs, systems documentation and software releases
  - Independence of quality assurance function
  - Integrity and security of the network, system and application software
  - Involvement of clients in the acquisition process

Support and Delivery

- Security administration
  - Formal policy & awareness program
  - Logical & physical security closely monitored
- Continuity planning
  - Comprehensive BCP
  - Plans current and tested
  - Pre-defined recovery time frames
- IT Operations
  - Consistent performance
  - Reliable processes
  - Available processes
  - End user / Customer support

Support and Delivery

- Support and delivery review includes adequacy of:
  - Operating policies, procedures, and manuals
  - Physical and logical security including data privacy
  - Security policies, procedures, and practices in all units and at all levels of financial institution
  - Service levels that meet business requirements
  - Data controls over preparation, input, processing, and output
  - Corporate contingency planning and business resumption
  - Programs/processes monitoring capacity/performance
  - Quality of assistance provided to users
  - Controls over and monitoring of OSPs
  - Firewall architectures/security of public networks