



FEDERAL DEPOSIT INSURANCE CORPORATION

Vendor Management

Outsourcing Technology Services

Objectives

Vendor Management – Outsourcing Technology Services

- **Board and Senior Management Responsibilities**
- **Risk Management Program**
 - Risk Assessment
 - Service Provider Selection
 - Contracts
 - Ongoing Monitoring
- **Business Continuity Planning and Testing**
- **Other Available Resources**

Board and Senior Management Responsibilities

Vendor Management – Outsourcing Technology Services

The Board can outsource a service, but cannot outsource the responsibility.

- **Develop and implement risk-based policies and procedures to govern the outsourcing process**



Board and Senior Management Responsibilities

Vendor Management – Outsourcing Technology Services

Board Responsibilities

- **Develop and approve policies that establish an effective vendor management program framework**
- **Select a service provider that best meets the needs of the bank**
- **Negotiate a contract that protects the interests of the bank**
- **Oversee management's implementation of the program through regular board reporting**

Board and Senior Management Responsibilities

Vendor Management – Outsourcing Technology Services

Board Reports

- **Audits**
- **Business Continuity Plans and Testing**
- **Service Level Agreements**
- **Information Security**
- **Financial Statements**
- **Higher-risk Service Providers**
- **Regulatory IT Examination Reports**

Board and Senior Management Responsibilities

Vendor Management – Outsourcing Technology Services

Management Responsibilities

- **Evaluate prospective providers based on the type of services outsourced and how critical the function is to the bank**
- **Ensure each outsourced relationship supports business requirements and strategic plans, and is appropriate for the size and complexity of the bank**
- **Confirm the bank has sufficient expertise to oversee and manage the relationship**
- **Implement ongoing monitoring programs that prioritize activities based on the degree of risk and criticality of the services**

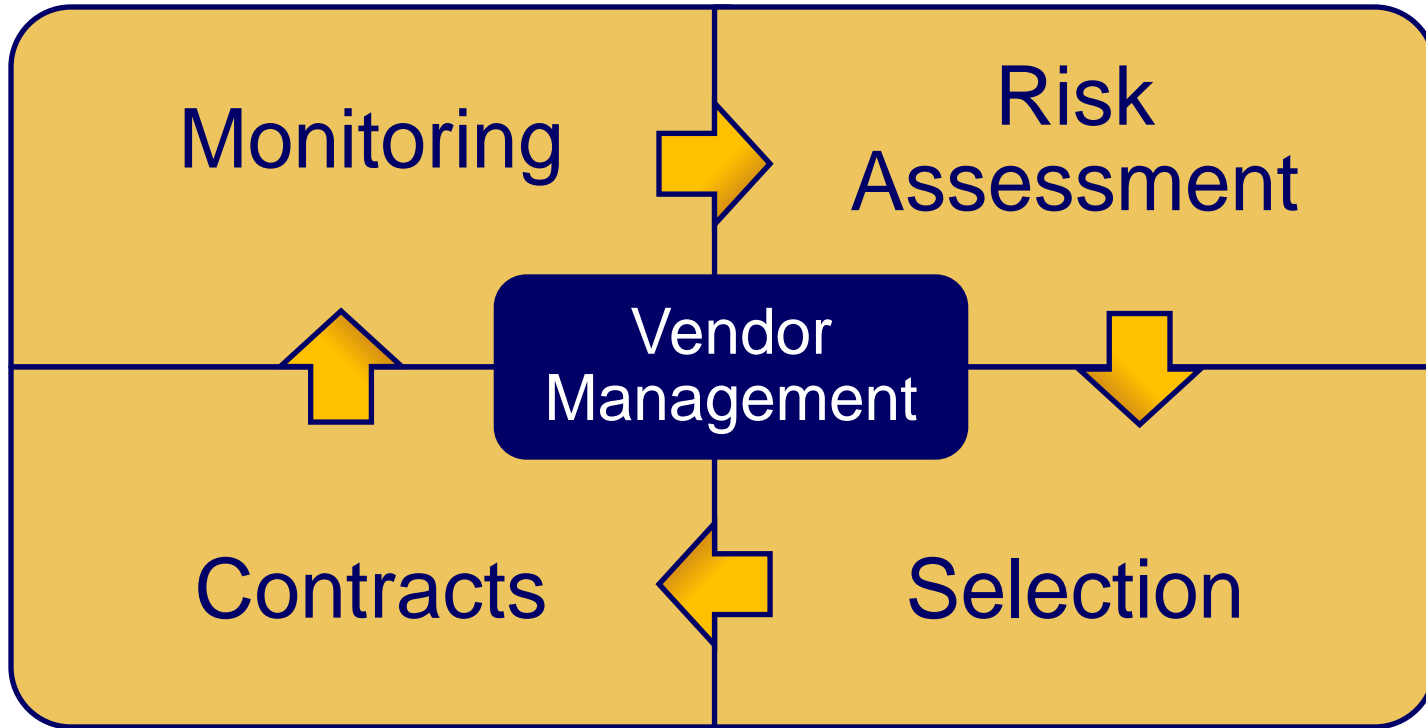
Risk Management Overview

Vendor Management – Outsourcing Technology Services

- **Inform senior management and the board of the risks associated with outsourcing**
- **Ensure that outsourcing arrangements are prudent and consistent with business objectives**
- **Implement effective controls to address identified risks**
- **Perform ongoing risk monitoring to identify and evaluate changes in risk from the initial assessment**
- **Document procedures, roles, responsibilities, and reporting mechanisms**

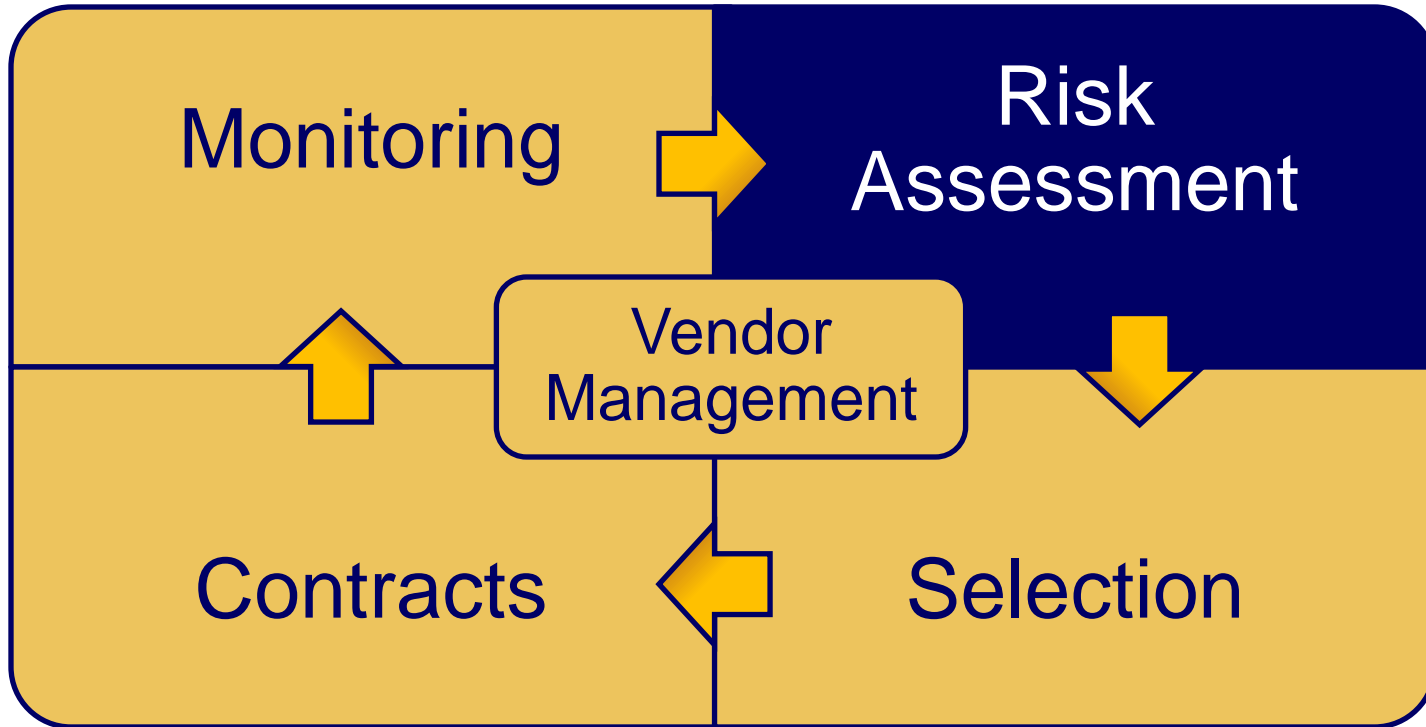
Risk Management Overview

Vendor Management – Outsourcing Technology Services



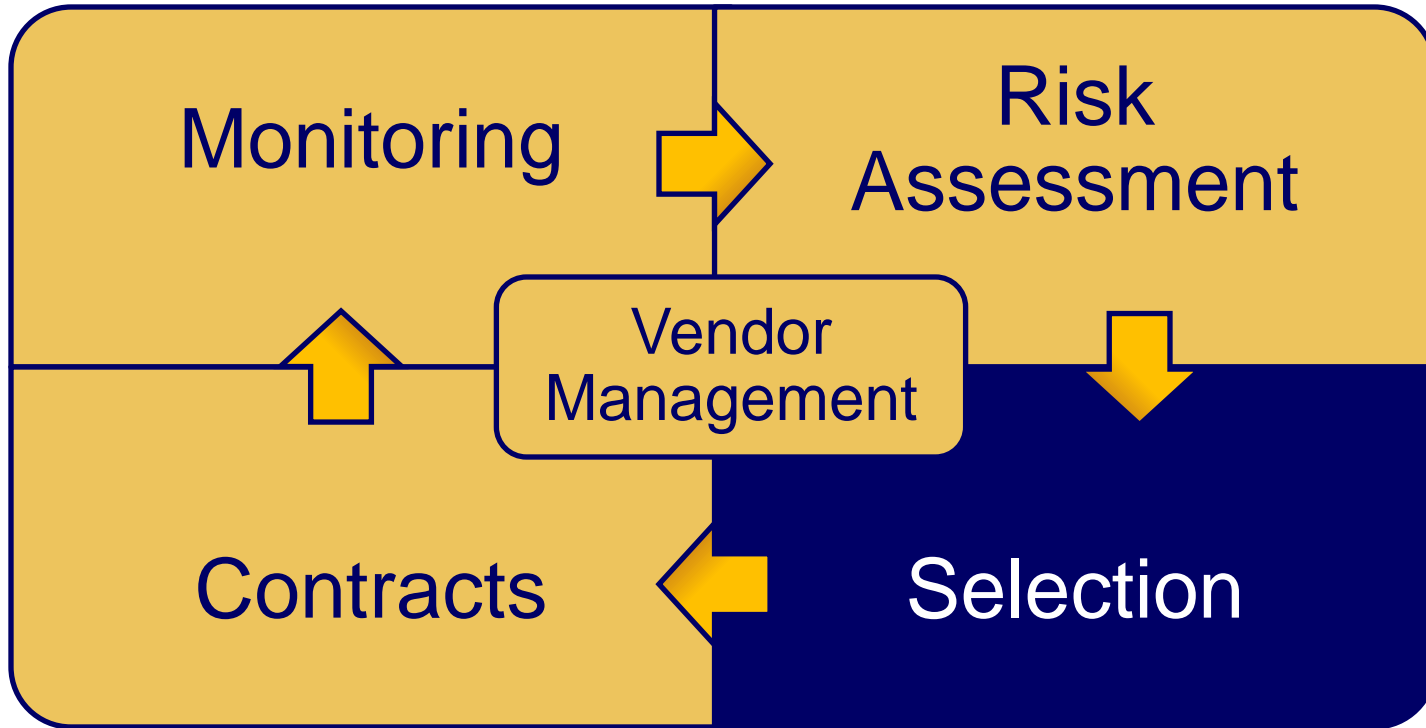
Risk Management Overview

Vendor Management – Outsourcing Technology Services



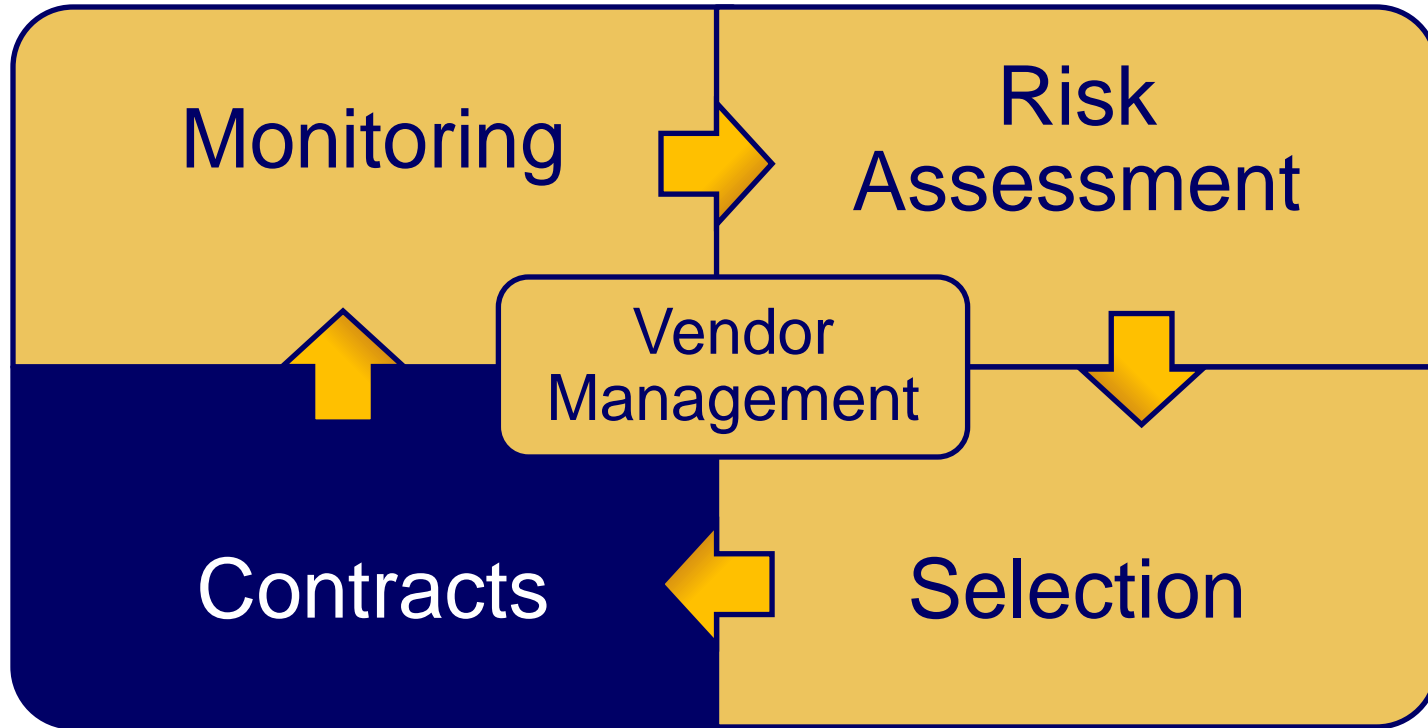
Risk Management Overview

Vendor Management – Outsourcing Technology Services



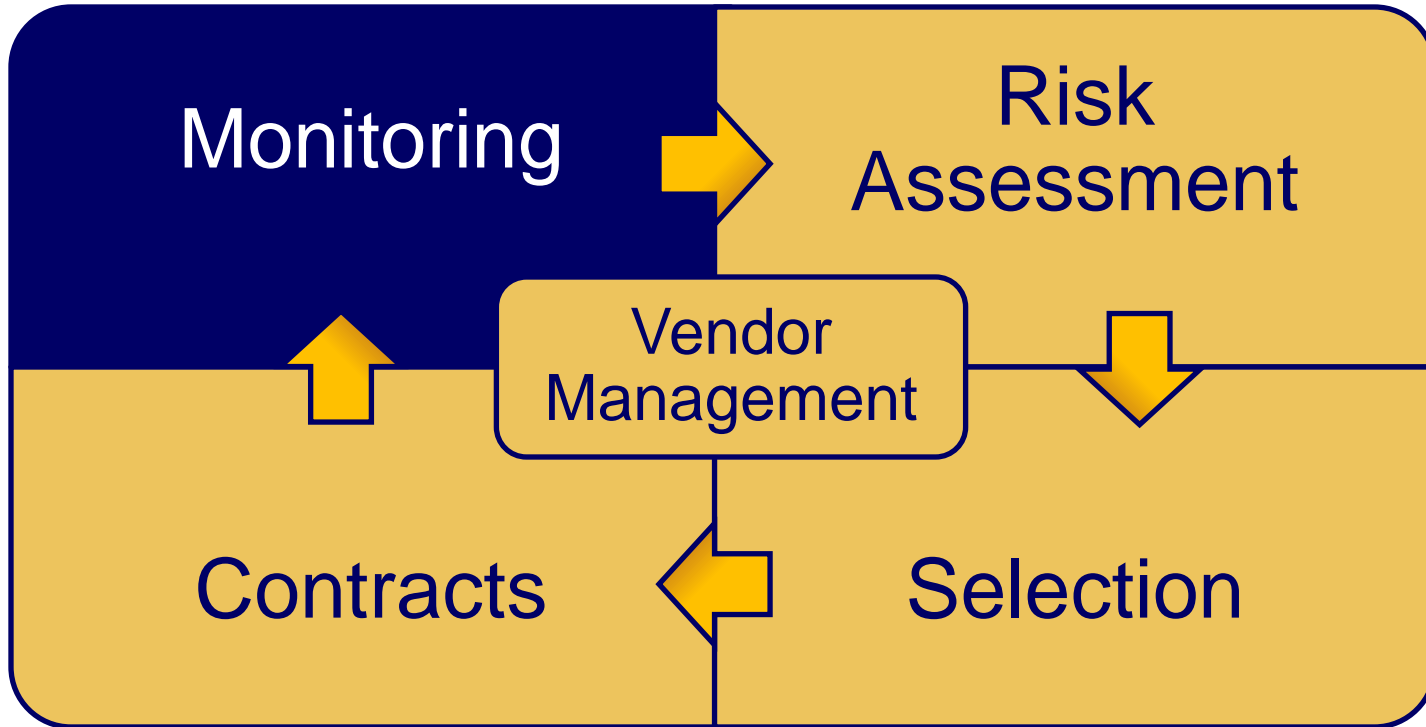
Risk Management Overview

Vendor Management – Outsourcing Technology Services



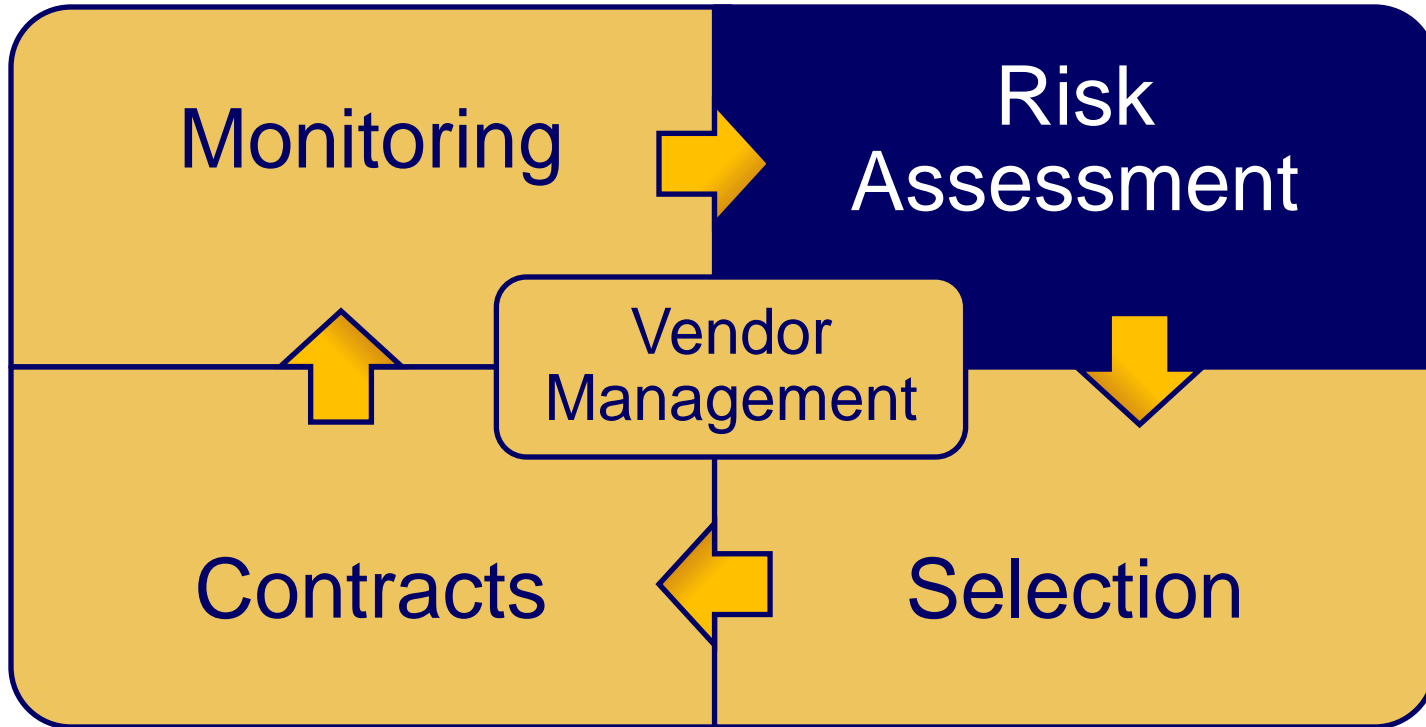
Risk Management Overview

Vendor Management – Outsourcing Technology Services



Risk Management Overview

Vendor Management – Outsourcing Technology Services



Risk Assessment

Vendor Management – Outsourcing Technology Services

Risks

Strategic

- Planning, implementation, scalability

Compliance

- Legal and regulatory requirements

Reputational

- Errors, delays, omissions, fraud, breaches

Interest Rate

- Errors, inaccurate assumptions

Liquidity

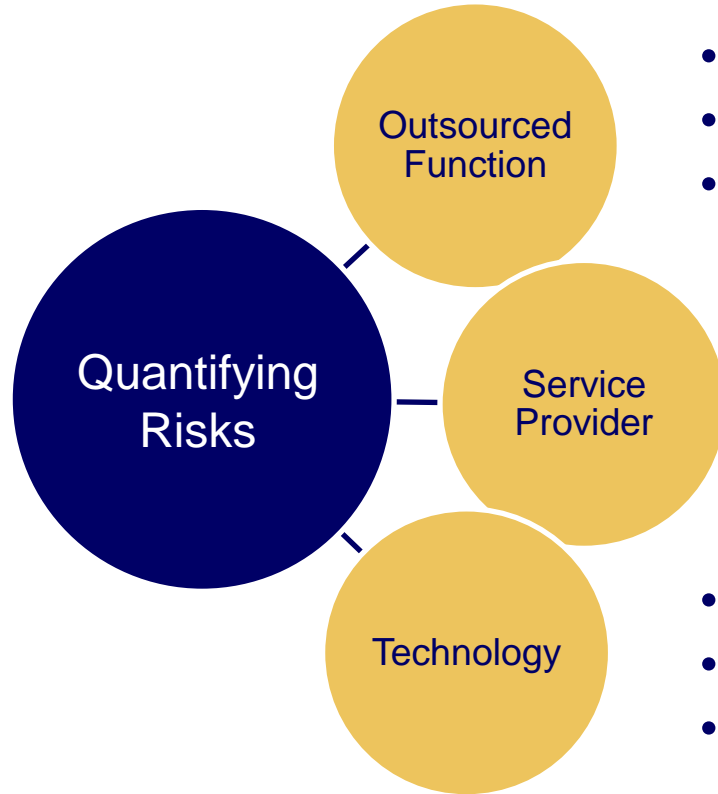
- Service disruptions, settlement delays

Cyber

- Disruption, malware

Risk Assessment

Vendor Management – Outsourcing Technology Services



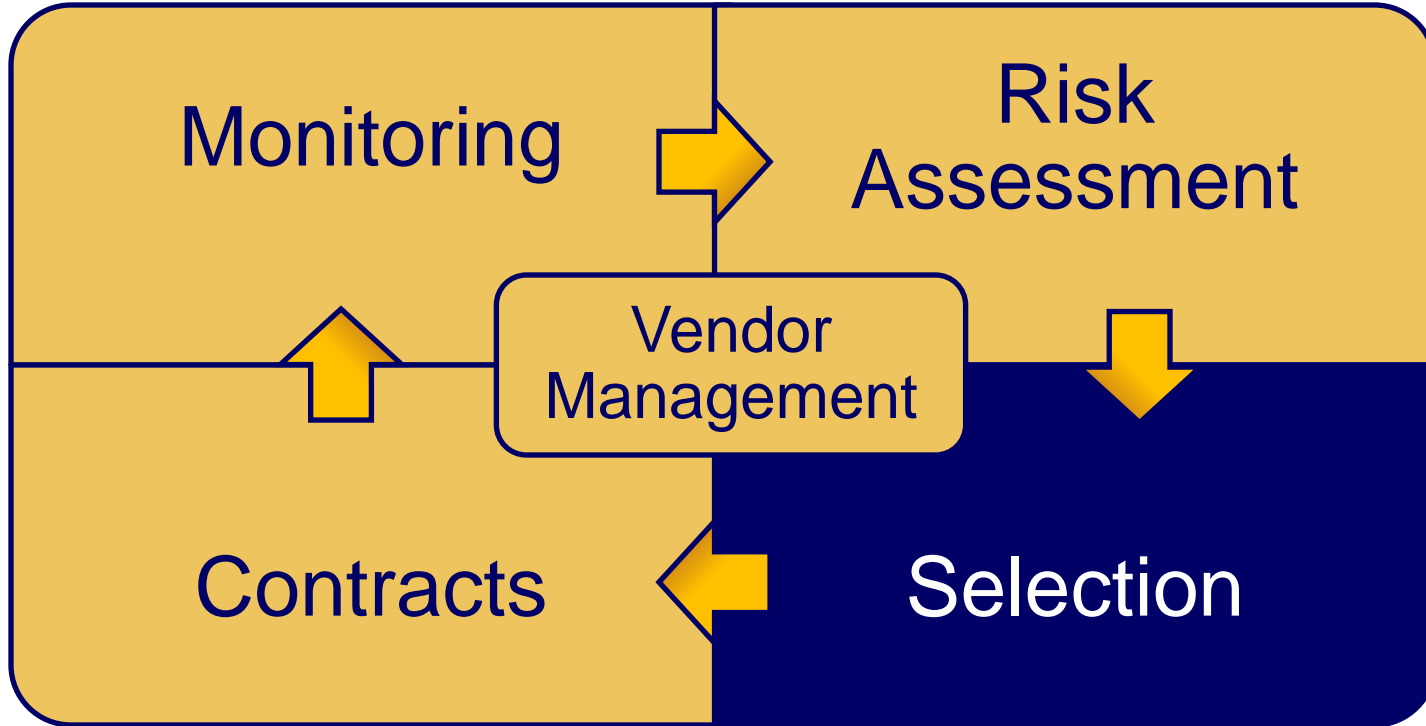
- Criticality
- Data sensitivity
- Transaction volume

- Financial strength
- Industry experience
- Location

- Reliability
- Security
- Scalability

Vendor Selection

Vendor Management – Outsourcing Technology Services



Vendor Selection

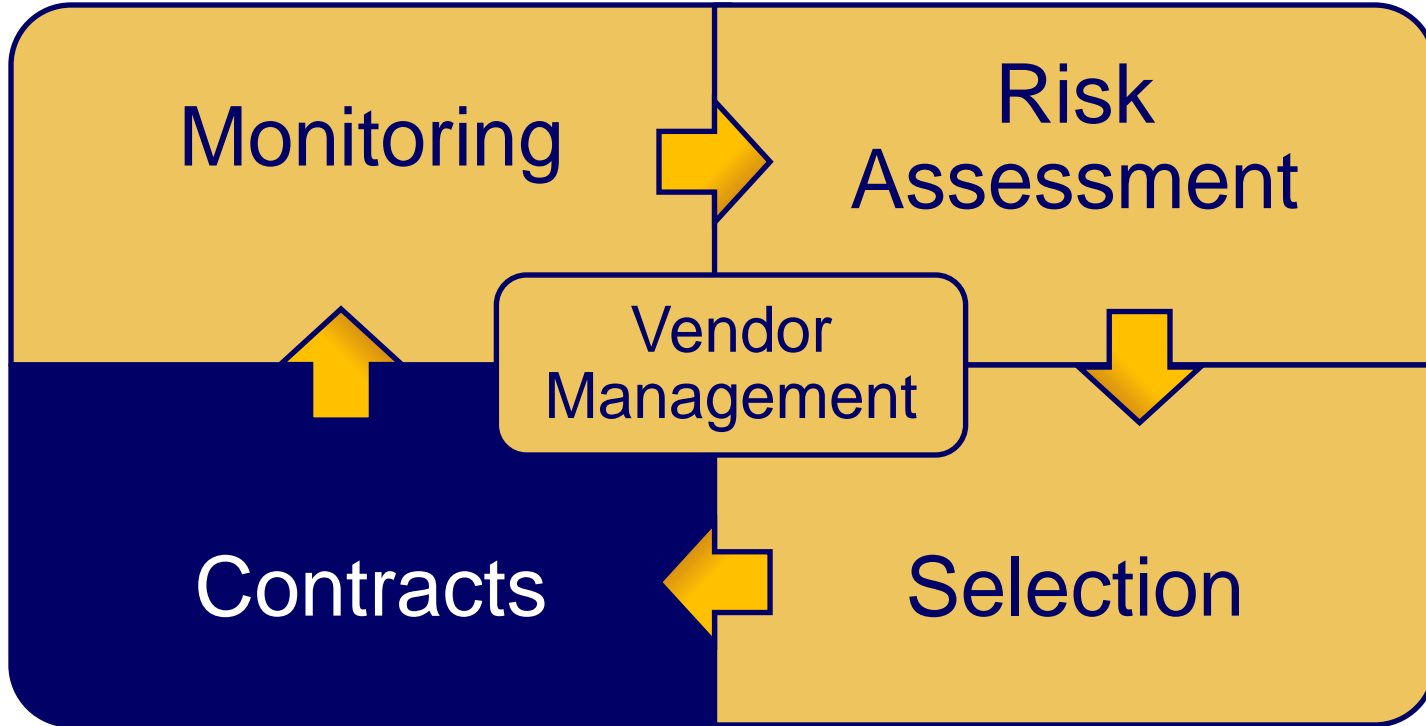
Vendor Management – Outsourcing Technology Services

Due Diligence: Key Considerations

- Corporate history, qualifications, references
- Financial condition
- Service delivery capability
- Technology and system architecture
- Internal control environment, security history, audit coverage
- Reliance on and success in managing subcontractors
- Legal and regulatory compliance
- Insurance coverage
- Site visits
- Disaster recovery/business continuity

Contracts

Vendor Management – Outsourcing Technology Services



Contracts

Vendor Management – Outsourcing Technology Services

Common Provisions

Scope of Service

- Rights and Responsibilities
 - *Description of Activities*
 - *Timeframes for Implementation*
 - *Assignment of Responsibilities*

Security and Confidentiality

- Responsibility and Controls
- Incident Response and Notification Requirements
- Appendix B to Part 364 (GLBA)

Contracts

Vendor Management – Outsourcing Technology Services

Common Provisions

Internal Controls

- Records Maintenance
- System Monitoring
- Notification Requirements
- Cybersecurity

Audit

- Types of Audits
 - *Financial*
 - *General Controls*
 - *Network Security Assessments*
 - *Electronic Funds Transfer*
 - *Disaster Recovery Tests*
- Frequency
- Right to Receive
- Right to Audit

Contracts

Vendor Management – Outsourcing Technology Services

Common Provisions

Reports

- Frequency and Types
 - *Performance*
 - *Financials*
 - *Compliance with regulatory guidance*

Business Resumption/ Contingency Plans

- Backup and Records Protections
 - *Equipment*
 - *Programs and Data Files*
- Maintenance and Testing
 - *Frequency*
 - *Availability of Test Results*
 - *Bank Participation*

Contracts

Vendor Management – Outsourcing Technology Services

Common Provisions

Sub-contracting

- Awareness
- Assessment
- Responsibility

Regulatory Compliance

- Adherence to Regulatory Guidance
 - *Risk Management*
 - *Consumer Compliance*

Performance Standards

- Measurable
- Minimum Service Level Requirements
- Remedies
- Service Level Agreements (SLAs)

Contracts

Vendor Management – Outsourcing Technology Services

Bank Service Company Act Notification

- **Banks should notify their primary Federal regulator of the outsourcing relationship within:**
 - 30 days of entering into the contract, or
 - performance of the services

.....whichever occurs first

Contracts

Vendor Management – Outsourcing Technology Services

SLAs

Confidentiality of Data

- GLBA compliance, notifications, responsiveness

Integrity and Availability

- Error rates, up time, processing timeliness

System Changes

- Programming changes, system updates

Security Standards

- Compliance, independent testing

Business Continuity

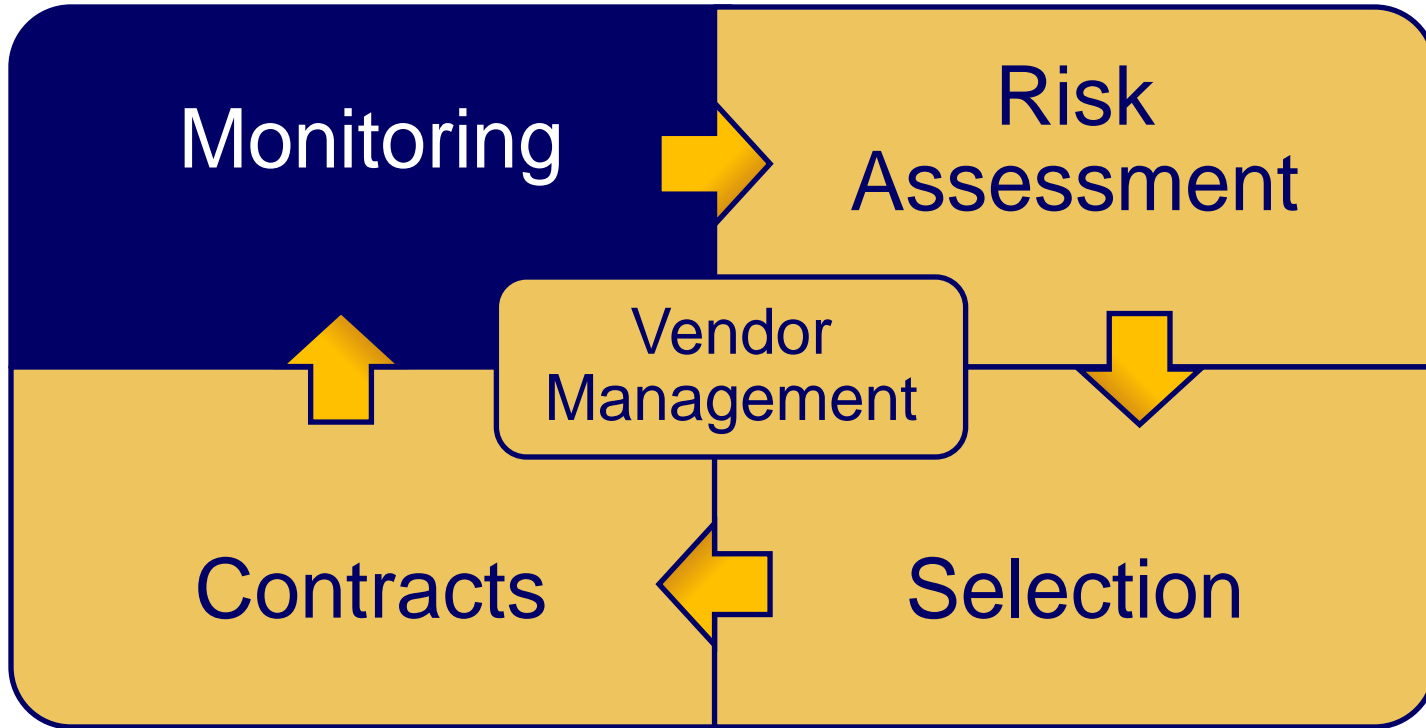
- Backup, retention, protection, restoration, recovery

Help Desk Support

- Responsiveness, availability, qualifications

Monitoring

Vendor Management – Outsourcing Technology Services



Monitoring

Vendor Management – Outsourcing Technology Services

- **Periodically reevaluate active service providers**
- **Tailor ongoing monitoring using a risk-based approach considering:**
 - Criticality of the services
 - Sensitivity of data
 - Degree of perceived risk
- **Implement more frequent and stringent ongoing monitoring for higher-risk service providers**
- **Report results to the board**

Monitoring

Vendor Management – Outsourcing Technology Services

■ Audit reports

- Performed by qualified and independent personnel
- Type, scope, and frequency consistent with:
 - Size and complexity
 - Products and services
 - Level of risk
- Review corrective actions



Monitoring

Vendor Management – Outsourcing Technology Services

- **Financial Condition**
 - Continuity of operations
 - Support for the contracted services
 - Investment in security controls
 - Product updates



Monitoring

Vendor Management – Outsourcing Technology Services

- **Compliance with Service Level Agreements**
 - Performance standards
 - Information security standards (GLBA)
 - Incident response programs
- **Business Continuity Plans**



Monitoring

Vendor Management – Outsourcing Technology Services

- Available only to client banks under contract
- Request from FDIC Regional Office Case Manager
- National and State-member banks may request from the bank's primary Federal regulator

*Interagency Examination of
Technology Service
Provider*

Your Technology Service Provider

THIS REPORT OF EXAMINATION IS STRICTLY CONFIDENTIAL

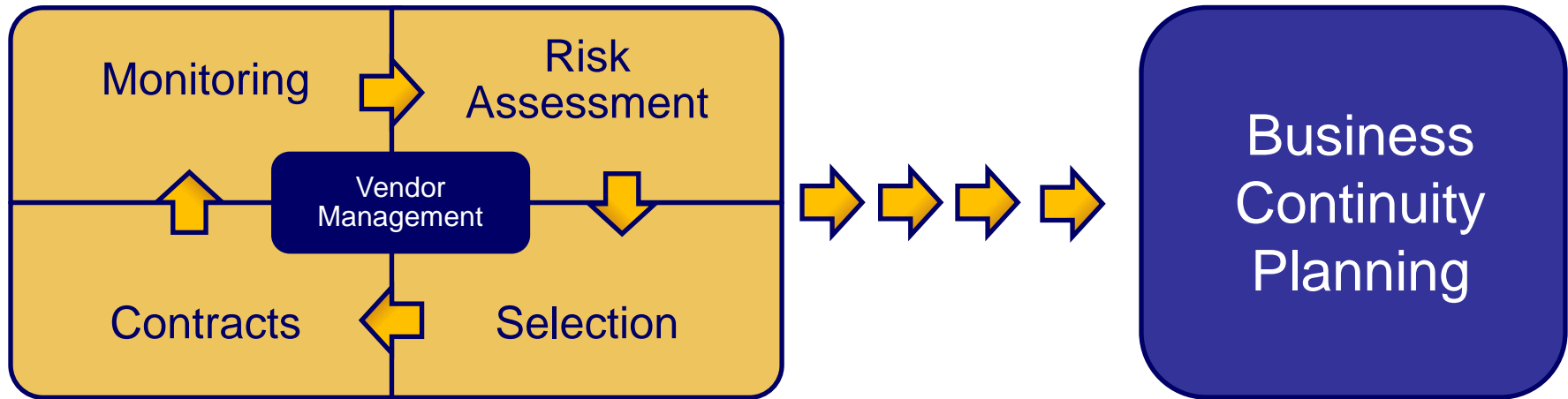
The report of examination is the property of the Federal Financial Institutions Examination Council and is provided for the confidential use of the examinee only. The information contained in this document is based upon the records and books of the entity, upon information readily accessible to others, and upon information obtained from other sources believed to be reliable and correct.

The examination is not an audit and should not be construed as such. It is emphasized that the examinee bears primary responsibility for the responsibility for making or providing for adequate records of the examined entity.

Under no circumstances shall any member of the report or any of its contents, either in whole or in part, be disclosed to any other person without the express written consent of the Federal Financial Institutions Examination Council. The examinee shall maintain the report and its contents in strict confidence and shall not disclose the report or its contents to any other person without the express written consent of the Federal Financial Institutions Examination Council. Form Date: June 2015

Business Continuity Planning

Vendor Management – Outsourcing Technology Services



Business Continuity Planning

Vendor Management – Outsourcing Technology Services

- **Review service provider plans**
 - Mission critical service restoration
 - Timeframes and recovery time objectives
 - Staffing, capacity, telecommunications, hardware, software, and facilities availability
 - Wide-scale disruptions
 - Contingency plan testing and testing scenarios
 - Connectivity, functionality, volume, and capacity of alternate facilities
 - Annual or more frequent
 - Interdependencies
 - Internal and external dependencies
 - Test where feasible

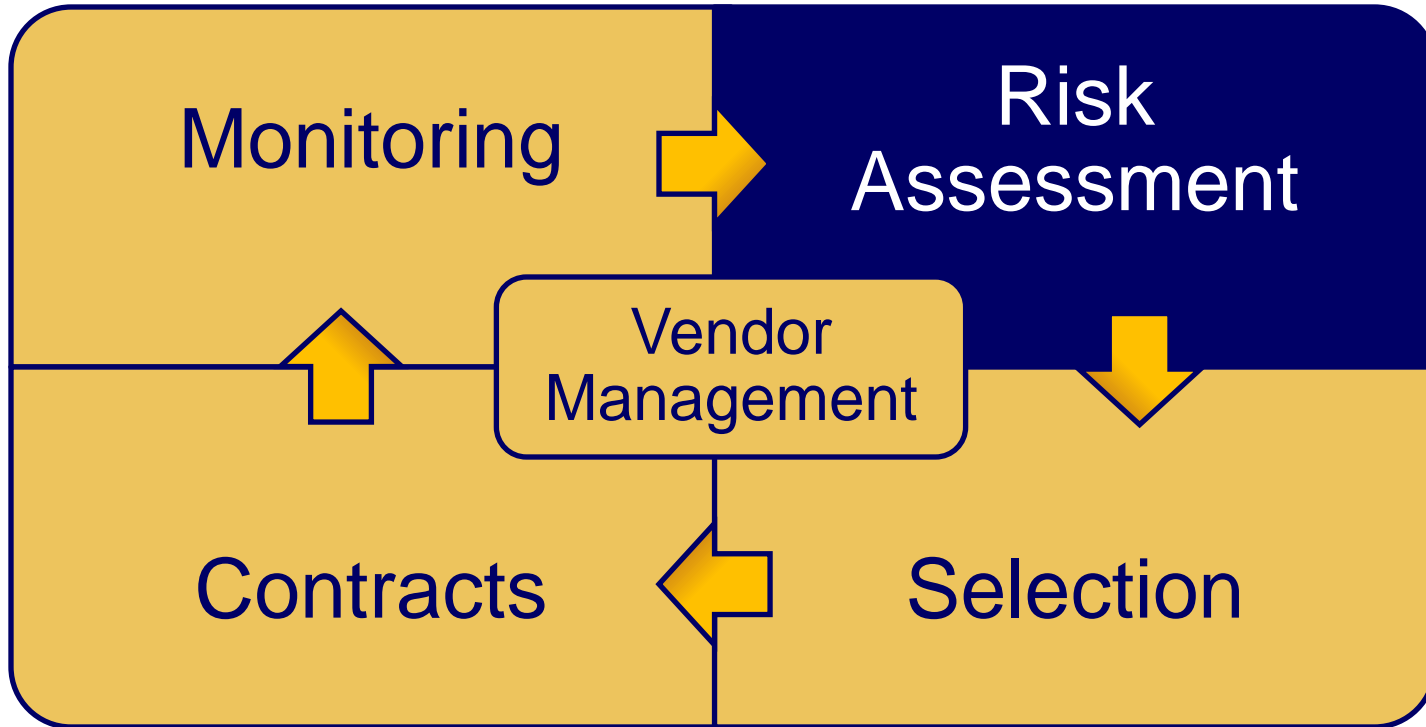
Outsourcing to Foreign Service Providers

Vendor Management – Outsourcing Technology Services

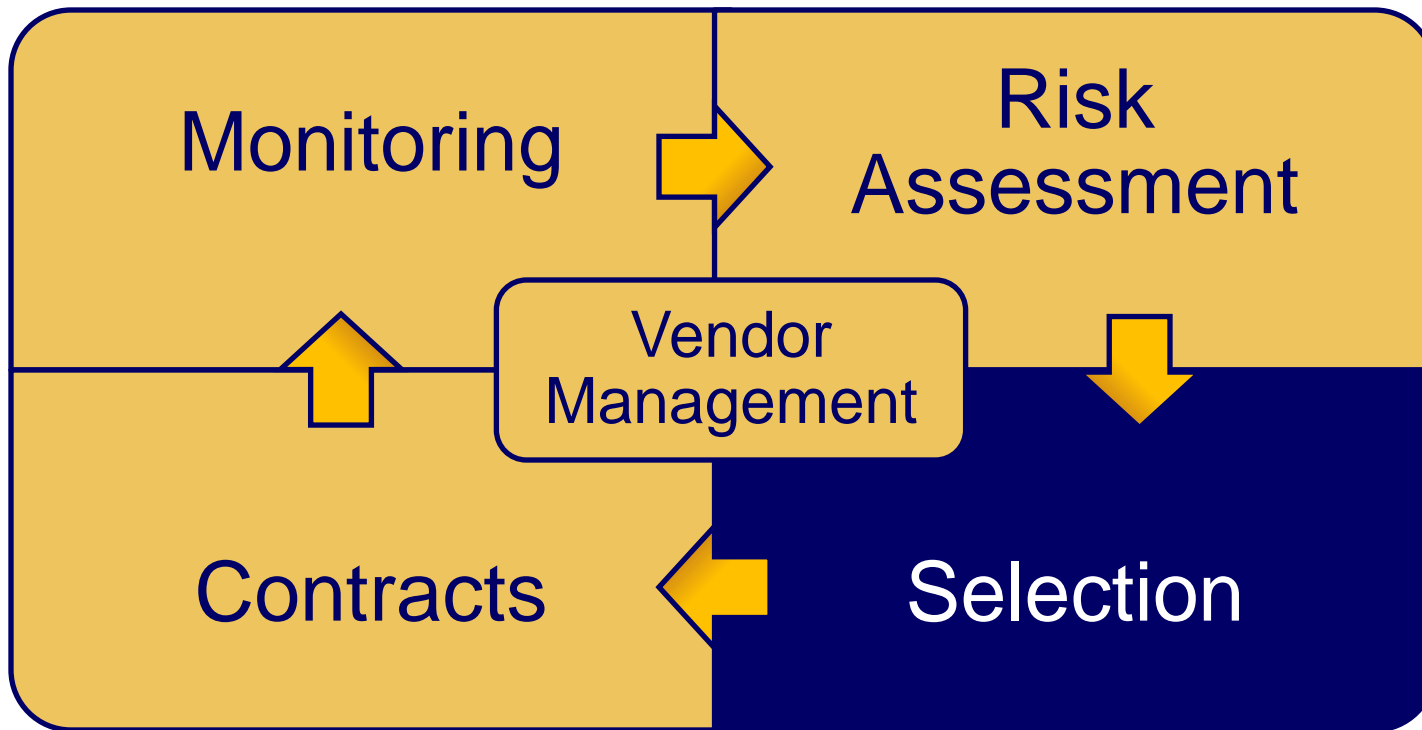
- Arrangements should be subject to the same due diligence and assessment processes as domestic outsourcing relationships
- Risks become unique



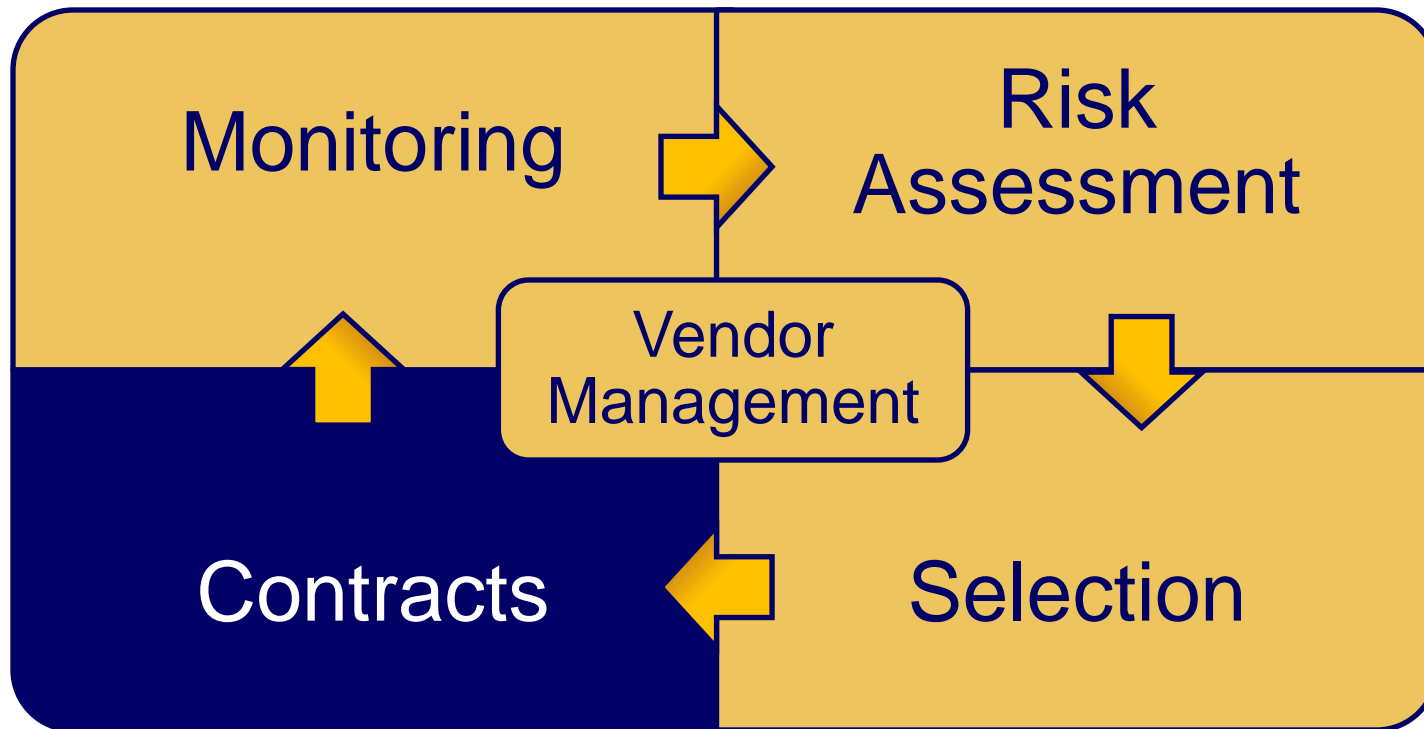
Summary: Review



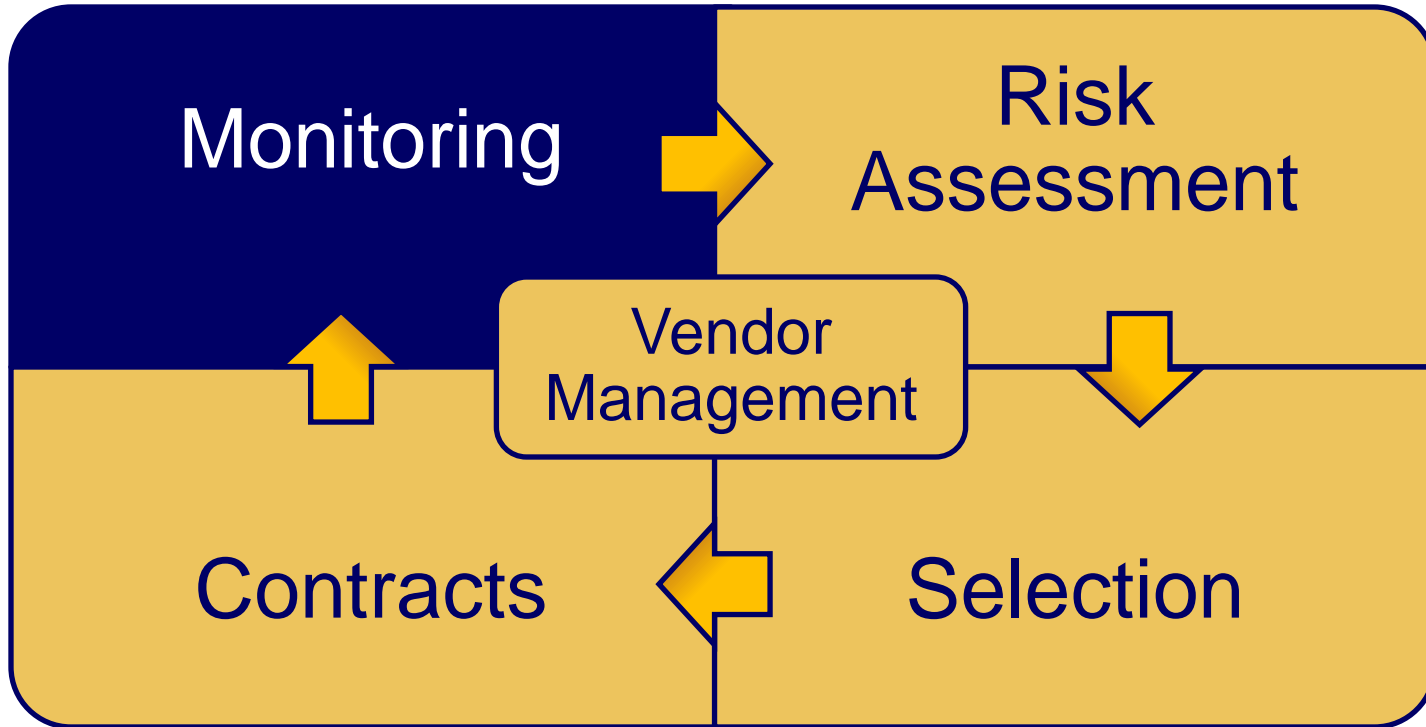
Summary: Review



Summary: Review



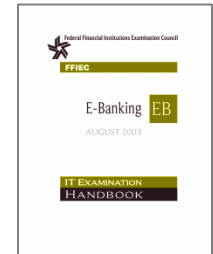
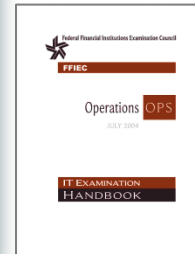
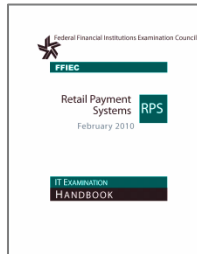
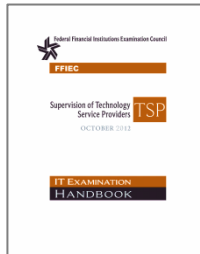
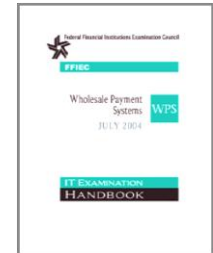
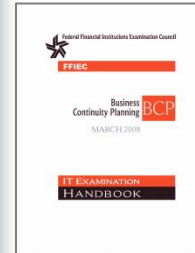
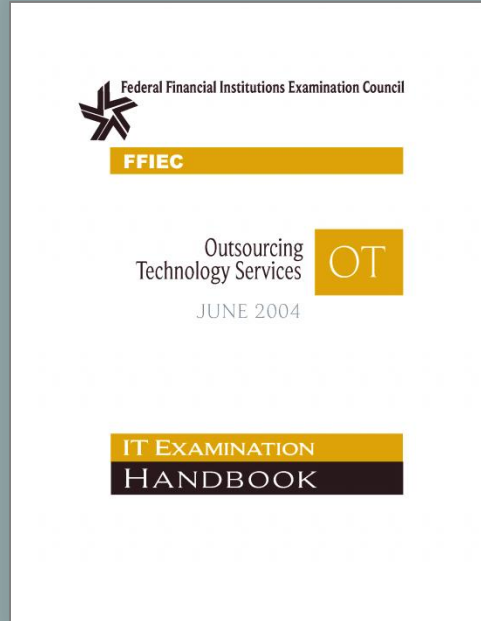
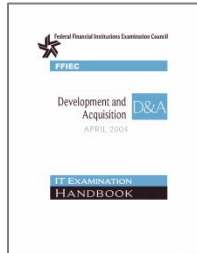
Summary: Review



Resources

Vendor Management – Outsourcing Technology Services

- **FFIEC IT Examination Handbook (www.FFIEC.gov)**



Resources

Vendor Management – Outsourcing Technology Services

- **FDIC Financial Institution Letters (FILs)**
 - FIL-13-2014: Informational Tools for Community Bankers
 - FIL-44-2008: Guidance for Managing Third-Party Risk
 - FIL-52-2006: Guidance on Foreign-Based Third-Party Service Providers
 - FIL-121-2004: Computer Software Due Diligence
 - FIL-23-2002: Country Risk
 - FIL-81-2000: Risk Management of Technology Outsourcing
 - FIL-49-99: Bank Service Company Act

Website: www.fdic.gov

Resources

Vendor Management – Outsourcing Technology Services

- Directors' Resource Center
www.fdic.gov/regulations/resources/director/

- Technical Assistance Video Program
 - Information Technology (IT)
 - Corporate Governance
 - Third-Party Risk
 - Cybersecurity Awareness
 - Cyber Challenge: A Community Bank Cyber Exercise

- Questions
supervision@fdic.gov