IT Examination Handbook Presentation
Outsourcing Technology Services Booklet

Visual Narrative

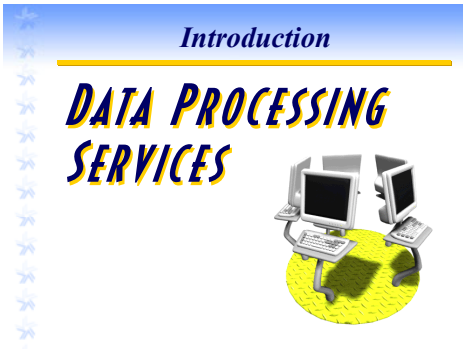
1.

Outsourcing technology services is covered only briefly in the 1996 FFIEC Information Systems Examination Handbook. This booklet expands on that coverage and includes information on topics related to this issue not in the 1996 Handbook.

2.

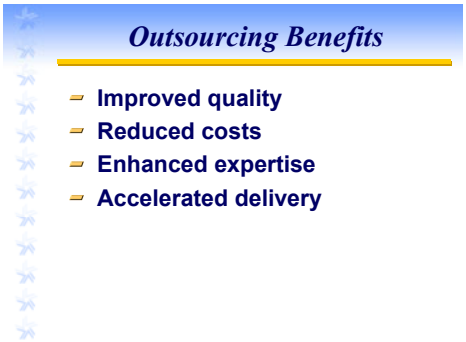
The booklet uses the term "outsourcing" to describe reliance on external service providers to carryout a variety of technology-related services; including tasks such as programming and data processing.

3.



As such practices have become common in financial institutions over the last few years, reviewing outsourced technology services has become a significant part of the IT examination process.

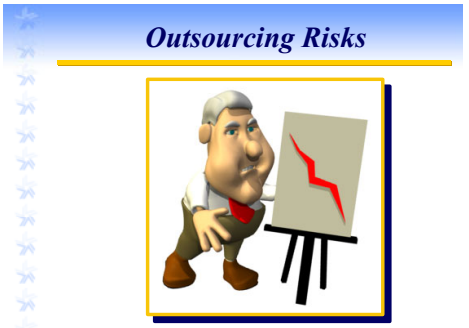
4.



Management at a particular financial institution may choose to outsource technology-related services for a variety of reasons—for example, improving quality, reducing costs, enhancing expertise, or accelerating the delivery of new products.

Visual Narrative

5.

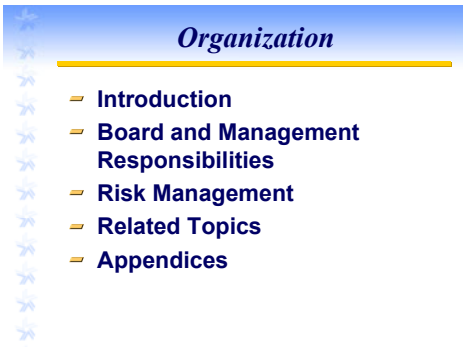


Regardless of the benefits it offers, outsourcing does not reduce the fundamental risks associated with information technology systems and applications or management's responsibilities to appropriately monitor and manage them.

6.

Furthermore, outsourcing may introduce new risks that are different from those resulting from technology-related functions that are conducted internally. Consequently, outsourcing may require different types of controls than those used internally.

7.



The booklet presents an overview of these controls in five sections:

- Introduction,
- Board and Management Responsibilities,
- Risk Management,
- Related Topics, and
- Appendices.

8.

Having covered a general introduction to outsourcing, let's now look at the Board and Management Responsibilities section of the booklet.

Visual Narrative

9.

The responsibility for overseeing the management of risks associated with outsourcing begins with the institution's board of directors and senior management

10.

who should ensure the development of an outsourcing oversight program to:

- Identify,
- Measure,
- Monitor, and
- Control

the risks associated with outsourcing on an enterprise-wide basis.

11.

The booklet looks at four different areas of risk management that are of particular importance in the outsourcing process:

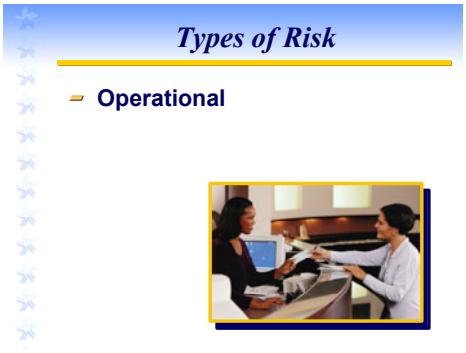
12.

- Risk assessment and requirements definitions,
- Service provider selection,
- Contract negotiation and implementation, and
- Ongoing monitoring.

Before we discuss these four control areas, let's first look at the type of risks faced by institutions engaged in outsourcing.

Visual Narrative

13.



Operational risk is the primary risk associated with outsourcing IT services and may arise from fraud, error, or the inability of a provider to deliver products that meet the requirements of the institution's operating procedures.

14.

Operational risk is a concern in all processes related to the delivery of an institution's financial products and services. This includes not only operations and transaction processing, but also areas such as customer service, systems development, and capacity planning.

15.

Reputation risk can arise as outsourcing literally means that management is staking the institution's reputation on services provided outside of its direct control.

16.

Strategic risk can occur if inaccurate information from a provider can cause even an experienced management team to make unsound decisions.

Visual Narrative

17.

Types of Risk

- Operational
- Reputation
- Strategic
- **Compliance**

Compliance risks occur when providers fail to meet the terms of the serviced institution's regulatory compliance obligations. For example a provider's unauthorized disclosure of confidential customer information. Such failures can subject the institution to legal sanctions and potential lawsuits from customers.

18.

Types of Risk

- Operational
- Reputation
- Strategic
- Compliance
- **Interest rate, liquidity, and price**

Interest rate, liquidity, and price risk can arise if processing errors related to functions such as investment income put a financial institution at risk from unidentified changes in interest rates or market prices.

19.

Quantity of Risk

- **Function**
- **Qualifications**
- **Technology**

The quantity of risk associated with each type of risk depends on several factors, including what function the financial institution is outsourcing, the qualifications and characteristics of the service provider, and the technology the provider is using. Management should consider all three of these factors from the very start of an outsourcing process.

20.

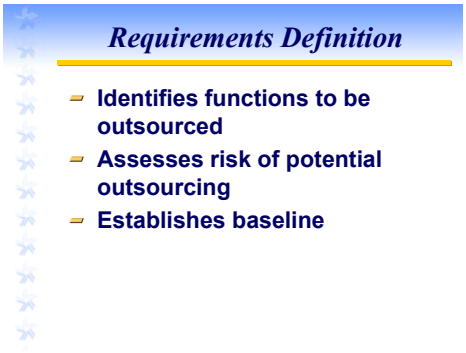
Risk Assessment

- **Quantity of Risk**
- **Requirements Definition**

In order to accurately assess the quantity of risk associated with a particular outsourcing relationship, management should clearly define specific requirements for the particular function it plans to outsource.

Visual Narrative

21.



A clear requirements definition is the cornerstone of effective risk management in the outsourcing environment, as it sets the stage for all of the activities that follow. Requirements definitions should be developed through a process that:

- Identifies the functions or activities to be outsourced
- Assesses the risk of outsourcing those functions or activities, and
- Establishes a baseline from which appropriate control measures can be identified.

22.

Key to the requirements definition process are:

- Stakeholder involvement,
- An integration process that supports solicitation, selection, contracting, and monitoring, and
- Sufficient documentation to ensure that the service delivered actually meets the institution's requirements.

23.

Sound planning techniques and a systematic approach to acquisition should lead to a requirements definition that spells out the specific:

- Scope of the products or services required,
- Standards and service levels that will be used to evaluate the products and or services that are provided;
- Minimum qualifications and acceptable characteristics for the service provider selected;
- Specific reporting requirements for the service provider;
- Methods for migration of data between the institution and the service provider at the beginning and end of the contract;
- Contract issues such as duration, termination, and dispute resolution; and
- Contractual protections, such as liability and insurance.

Visual Narrative

24.

Risk Management

- Risk Assessment and Requirements
- **Service Provider Selection**
- Contract Issues
- Ongoing Monitoring

After discussing the basic parameters necessary for conducting effective risk assessment and developing a well-defined set of project requirements, the booklet looks at the actual process for selecting service providers.

25.

Service Provider Selection

Service provider selection typically starts with a request for proposal, or RFP, that is based primarily on information developed during the risk-assessment and requirements phase.

While the level of detail may vary for any particular procurement, the RFP should reflect a level of detail that ensures the institution has clearly stated all of its requirements and provides a sound basis for comparing responses from different service providers.

26.

Due Diligence

- **Verification**
- **Analysis**

Management should apply due-diligence techniques to the RFP responses it receives. This process should include verification and analysis of the proposals to ascertain which service providers can truly meet the institution's specific needs.

27.

Due Diligence

- **Human resource policies**
- **Service philosophies**
- **Quality initiatives**
- **Policies**
- **Culture, values, and business styles**

The evaluation team should also probe for information on intangibles as well as the technical aspects of the proposals. Issues such as the service provider's:

- Human resource policies,
- Service philosophies,
- Quality initiatives, and
- Policies for managing costs and improving efficiencies.

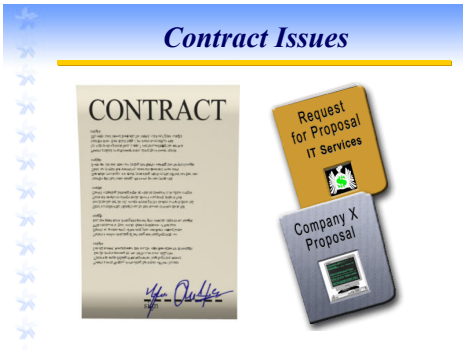
should be reviewed closely, and the evaluation team should ensure the culture, values, and business styles of potential service providers fit those of the financial institution as closely as possible.

Visual Narrative

28.

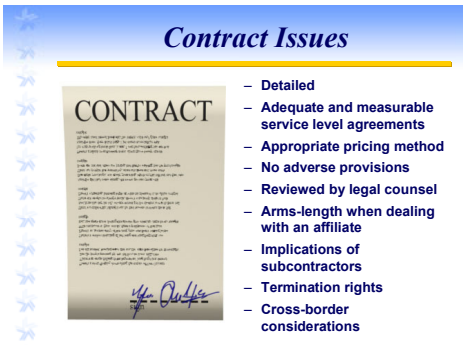
Once due diligence is performed, institutions typically enter into contract negotiations with one or more of the service providers that demonstrate an ability to meet the institution's requirements.

29.



The contract is typically negotiated using the RFP and the service provider's proposal as a starting point. The contract is the single most important control in the outsourcing process, and management should ensure that the contract:

30.



- Is detailed enough to thoroughly define the rights and responsibilities of both parties;
- Contains adequate and measurable service level agreements;
- Is based on the most appropriate pricing method;
- Does not contain provisions or inducements that may adversely affect the institution;
- Is reviewed by competent legal counsel;
- Is on an arms-length basis when engaging the services of an affiliate;
- In the case of subcontracting relationships, that responsibility remains with the primary provider;
- Contains adequate exit or termination clauses; and
- Considers unique risks relating to contracting with a cross-border service provider when appropriate.

Visual Narrative

31.

Contract Elements

- Controls
- Audit procedures
- Business resumption plans

In addition to defining significant contract elements such as controls, audit procedures, and business resumption plans, the booklet provides more detailed information on four important aspects of the contracting process:

32.

Contract Issues

- Service level agreements

- Service-level agreements, which encapsulate the institution's requirements in a way that encourages the service provider to meet or exceed requirements and protects the institution if those requirements are not met;

33.

Contract Issues

- Service level agreements
- Pricing methods
  - Cost plus
  - Fixed price
  - Unit pricing
  - Variable pricing
  - Incentive-based pricing

- Pricing methods, which may include any of five primary methods:
  - Cost plus
  - Fixed price
  - Unit pricing
  - Variable pricing
  - Incentive-based pricing;

34.

Contract Issues

- Service level agreements
- Pricing methods
- Bundling

- Bundling, a process used by some providers to entice an institution to purchase more than one system, process, or service for a single price and which may or may not be to the benefit of the financial institution; and finally;

Visual Narrative

35.

- Contract inducements, which may offer the financial institution a short-term benefit but which may have adverse affects in the long term.

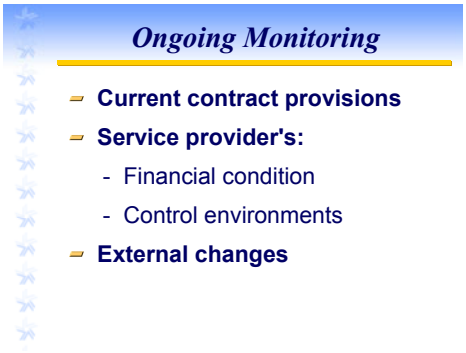
36.

Establishing requirements, selecting a service provider, and signing a contact are only the beginning of management responsibilities in the outsourcing environment. Management must continually monitor:

37.

- Service-provider compliance with the requirements outlined in active outsourcing contracts; and
- Changes that may create a need to modify outsourcing requirements.

38.



Effective monitoring should include reviews of:

- The key service level agreements and contract provisions currently in effect,
- The service providers' financial condition and general control environments, and
- Changes in the external environment that may require changes to outsourced services or products—for example, changes in regulations, the economic environment, or competition may require updates to the contract or service-level agreements.

Visual Narrative

39.

Organization

- Introduction
- Board and Management Responsibilities
- Risk Management
- **Related Topics**
- Appendices

Following a discussion on risk management, the booklet provides information on five "related topics" that are important in the outsourcing process:

40.

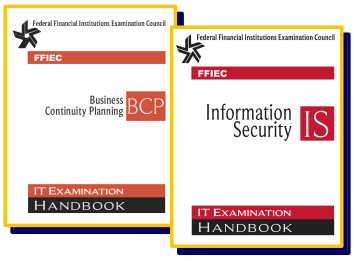
Related Topics

- **Information security**
- **Business continuity planning**
- **Business continuity outsourcing**
- **Multiple-provider relationships**
- **Foreign service providers**

- Information security and the process of safeguarding institutional and customer information and assets,
- Business continuity planning,
- The outsourcing of business continuity functions,
- Multiple service-provider relationships, and
- Outsourcing to foreign service providers.

41.

BCP & InfoSec



The *FFIEC IT Handbook* Business Continuity Planning Booklet and Information Security Booklet discuss detailed requirements for these two respective topics.

42.

Related Topics

- **Business continuity planning**
- **Information security**
- Outsourcing the business continuity function
- Multiple service provider relationships
- Foreign service providers

However, these two issues are equally important in the outsourcing environment, and the booklet looks at the special considerations required when monitoring third-party providers.

Visual Narrative

43. *Related Topics*

- Business continuity planning
- Information security
- **Outsourcing the business continuity function**
- Multiple service provider relationships
- Foreign service providers

When financial institutions outsource all or part of their business continuity capability,

44. *Outsourcing BC Functions*

management should consider a specific set of issues unique to that particular type of outsourcing. The booklet provides a broad list of these issues; including items such as processing time, testing, workspace, and staffing considerations.

45. *Related Topics*

- Business continuity planning
- Information security
- Outsourcing the business continuity function
- **Multiple-provider relationships**
- Foreign service providers

Multiple-provider relationships arise when two or more providers collaborate to deliver an end-to-end solution. An institution can select one of two techniques to manage these types of relationships:

46. *Multiple-provider Relationships*

- **Lead service provider**
- **Operating agreements**

- Use of a lead provider to manage the service providers involved in the end-to-end solution; or
- Establish operating agreements between each of the service providers or stand-alone contracts.

Visual Narrative

47.

Related Topics

- Business continuity planning
- Information security
- Outsourcing the business continuity function
- Multiple-provider relationships
- **Foreign service providers**

The final issue covered in the booklet's related topics section is Outsourcing to Foreign Service Providers.

48.

Foreign Service Providers

Financial institutions increasingly consider foreign-based third parties, or domestic firms that subcontract portions of their operations to foreign-based entities, as a resource for functions such as code development and data processing.

49.

Foreign Service Providers

- **Compliance**
- **Contractual**
- **Reputational**
- **Operational**
- **Strategic**

Although foreign-based service providers are now a common business practice, outsourcing to foreign countries raises country-specific compliance, contractual, reputational, operational, and strategic issues that require unique risk-management considerations.

50.

Organization

- Introduction
- Board and Management Responsibilities
- Risk Management
- Related Topics
- **Appendices**

The appendices include the standard Appendix A, which details Examination Procedures, and Appendix B, which includes references. Appendix C offers additional information on managing foreign-based third-party service providers.

Visual Narrative

51. *Exam Procedures*

The examination procedures are designed to assist examiners in evaluating the management processes used by an institution as it selects, monitors, and maintains ongoing relationships with third-party service providers.

52. *Foreign-Based Providers*

In managing foreign outsourcing relationships, management must consider not only the risk management practices applicable to domestic providers as discussed throughout the booklet, but also address the unique issues brought about by dealing with entities based in other countries.

53. *Appendix C*

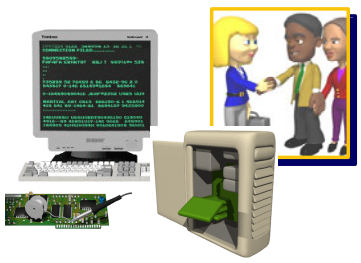
- **Country risk**
- **Compliance risk**
- **Due diligence**
- **Contracts**
- **Monitoring and oversight**
- **Regulatory agency access to information**
- **Examination considerations**

Appendix C provides discussion of some of these unique issues as they relate to,

- Country risk,
- Compliance risk,
- Due diligence,
- Contracts,
- Monitoring and oversight,
- Regulatory agency access to information, and
- Examination considerations

in the monitoring and ongoing oversight of foreign-based providers.

54. *Conclusion*



And, perhaps the latter phrase is the key to successfully applying the information presented in the Outsourcing Technology Services Booklet—critical to managing risks associated with third-party service providers is an understanding that these are, in fact, ongoing relationships that require continued and systematic monitoring.