



TECHNOLOGY SERVICE PROVIDER AND SERVICE RECEIVER

October 2007

**Essential Practices for Information Technology
Examination Manual
IT Section**

FCA Essential Practices for Information Technology

Based on Industry Standards and FFIEC Examination Guidance

Table of Contents

	Page
Technology Service Provider and Service Receiver	
Introduction	<u>SPR - 1</u>
Examination Objectives.....	<u>SPR - 1</u>
Examination Procedures	<u>SPR - 1</u>
<u>Essential Practice Statements</u>	<u>SPR - 2</u>
Risk Assessment.....	<u>SPR - 2</u>
Due Diligence	<u>SPR - 2</u>
Contract.....	<u>SPR - 2</u>
Monitoring.....	<u>SPR - 3</u>

Technology Service Provider and Service Receiver

Introduction:

The intense competition in the financial services industry has caused institutions to actively seek ways to cut costs and focus on their primary business. The rapid changes in information systems technology have caused many institutions to contract with third-party organizations for information processing, including mission critical applications. This interchange of services between organizations involves certain risks and responsibilities that must be addressed by both the service provider and receiver. While some of these can be defined and delegated within the service level agreement, others must be handled by each party through the implementation of proper operational controls. Legal counsel who is familiar with the terminology and specific requirements of a data processing contract should review it to protect the institution's interests and avoid or minimize problems in the contractual arrangement. This may require hiring legal counsel with specialization in IT issues.

Examination Objectives:

Determine if the board and management have established and maintained effective controls for technology services provided or received. This is accomplished through the following examination objectives:

- **Board and Management Oversight** – Assess the adequacy of board and management's risk assessment and due diligence efforts.
- **Contract Management** – Evaluate contracts and service level agreements to ensure technology service provider and receiver expectations are clearly defined.
- **Performance Monitoring** – Assess management's ongoing monitoring of the technology service provider or receiver and related contracts.

Examination Procedures:

Examination activities should be based on the criticality and complexity of the business functions present at the institution. The examination should begin with a review of audit activities and the risk assessment for technology service providers and receivers. At a minimum, the Essential Practices for Technology Service Providers and Receivers should be clearly documented and functioning within the internal control environment. More in-depth examination procedures (such as those found in the [FFIEC Supervision of Technology Service Providers Booklet](#) and the [Outsourcing Technology Services Booklet](#)) should be evaluated and incorporated into the examination scope as an institution's size, risk, and complexity increases.

Technology Service Provider and Service Receiver

Element		
Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Risk Assessment		
<p>Conduct a risk assessment to ensure an outsourcing relationship is consistent with an institution's short- and long-term goals. A risk assessment considers:</p> <ul style="list-style-type: none"> • Strategic goals and objectives of the institution; • Staff's ability to oversee outsourcing relationships; • Importance of the services to the institution; • Contractual obligations and requirements for the service provider; • Contingency plans, including availability of alternative service providers, costs and resources required to switch service providers; and • Necessary controls and reporting processes. <p><u>Reason:</u> <i>The board of directors and senior management are responsible for understanding the key risks associated with outsourcing arrangements and ensuring that effective risk management practices are in place.</i></p>	<p>FCA Informational Memorandum, "Risk Management of Outsourcing" (Oct. 25, 2000).</p>	<p>Outsourcing Technology Services Booklet (Jun. 2004), p. 5.</p> <p>Audit Booklet (Aug. 2003), pp. 21-22.</p> <p>Supervision of Technology Service Providers Booklet (Mar. 2003), pp. 1, 4-5.</p> <p>Management Booklet (Jun. 2004), p. 32.</p> <p>Information Security Booklet (Jul. 2006) pp. 76-77.</p>
Due Diligence		
<p>Perform and document due diligence to ensure technology service providers are managed adequately, competent technically, stable financially, and insured appropriately.</p> <p><u>Reason:</u> <i>Performing the due diligence allows management to evaluate service providers to determine their ability, both operationally and financially, to meet the institution's needs. Insurance coverage provided by the service provider should complement and supplement the institution's coverage. The coverage should be reviewed to determine if it is adequate and consistent with what the institution would have purchased without an external provider. Where the service provider's coverage is not sufficient, the institution should consider obtaining additional coverage.</i></p>	<p>FCA Informational Memorandums, "Outsourcing of Technology-related Products and Services" (Jan. 16, 2001); "Risk Management of Outsourcing" (Oct. 25, 2000).</p>	<p>Outsourcing Technology Services Booklet (Jun. 2004), p. 11.</p> <p>Supervision of Technology Service Providers Booklet (Mar. 2003), p. 6.</p> <p>Management Booklet (Jun. 2004), pp. 22, 32, 36.</p> <p>Information Security Booklet (Jul. 2006) pp. 76-78.</p>
Contract		
<p>Include the following elements in the written contract:</p> <ul style="list-style-type: none"> • Quality measures (Service Level Agreements or 	<p>ISO/IEC 17799:2000, Section 4.2.2, "Security Requirements in Third</p>	<p>Outsourcing Technology Services Booklet (Jun. 2004),</p>

Technology Service Provider and Service Receiver

Element		
Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
<p>minimum levels of service);</p> <ul style="list-style-type: none"> • Pricing; • Data ownership and confidentiality; • Right to audit (by institution and FCA); • Control expectations (i.e., security, change control, systems development, etc.); • Remediation; and • Reporting expectations for the Technology Service Provider to the institution. <p>Reason: <i>Documenting these measures ensures the institution's interests are protected, misunderstandings are minimized, and ongoing service is provided that is consistent with expectations.</i></p>	<p>Party Contracts.”</p>	<p>pp. 12-19</p> <p>Supervision of Technology Services Booklet (Mar. 2003), p. 1.</p> <p>Management Booklet (Jun. 2004), pp. 34, 36-38.</p> <p>E-Banking Booklet (Aug. 2003), pp. 23-24.</p>
Monitoring		
<p>Perform and document reviews of service provider's financial information, internal audit reports (e.g., SAS 70), status reports, and service level agreement reports.</p> <p>Reason: <i>It is essential that institutions implement an oversight program to monitor each service provider's controls and performance. Although services may be outsourced to achieve certain benefits, the responsibility for outsourced activities remains with FCS institutions' boards of directors. Documenting the process is important for contract negotiations, termination issues, and contingency planning. Specific personnel should be assigned responsibility for monitoring and managing the service provider relationship. The number of institution personnel assigned and the amount of time devoted to oversight activities will depend in part on the scope and complexity of the services outsourced.</i></p>	<p>FCA Informational Memorandums, “Outsourcing of Technology-related Products and Services” (Jan. 16, 2001); “Risk Management of Outsourcing” (Oct. 25, 2000).</p>	<p>Outsourcing Technology Services Booklet (Jun. 2004), pp. 20-24</p> <p>Supervision of Technology Service Providers Booklet (Mar. 2003), p. 6.</p> <p>Management Booklet (Jun. 2004), pp. 36-38.</p> <p>Audit Booklet (Aug. 2003), pp. 24-27.</p> <p>Information Security Booklet (Jul. 2006) pp. 76-78.</p>