Federal Financial Institutions Examination Council

2000 K Street, NW, Suite 310 . Washington, DC 20006 . (202) 872-7500 . FAX (202) 872-7501

Risk Management of Outsourced Technology Services

November 28, 2000

Purpose and Background

This statement focuses on the risk management process of identifying, measuring, monitoring, and controlling the risks associated with outsourcing technology services.[1] Financial institutions should consider the guidance outlined in this statement and the attached appendix in managing arrangements with their technology service providers.[2] While this guidance covers a broad range of issues that financial institutions should address, each financial institution should apply those elements based on the scope and importance of the outsourced services as well as the risk to the institution from the services.

Financial institutions increasingly rely on services provided by other entities to support an array of technology-related functions. While outsourcing to affiliated or nonaffiliated entities can help financial institutions manage costs, obtain necessary expertise, expand customer product offerings, and improve services, it also introduces risks that financial institutions should address. This guidance covers four elements of a risk management process: risk assessment, selection of service providers, contract review, and monitoring of service providers.[3]

Risk Assessment

The board of directors and senior management are responsible for understanding the risks associated with outsourcing arrangements for technology services and ensuring that effective risk management practices are in place. As part of this responsibility, the board and management should assess how the outsourcing arrangement will support the institution's objectives and strategic plans and how the service provider's relationship will be managed. Without an effective risk assessment phase, outsourcing technology services may be inconsistent with the institution's strategic plans, too costly, or introduce unforeseen risks.

---

[1] The *FFIEC Information Systems Examination Handbook* is a reference source that contains further discussion and explanation of a number of concepts addressed in this FFIEC guidance.

[2] Technology service providers encompass a broad range of entities including but not limited to affiliated entities, nonaffiliated entities, and alliances of companies providing products and services. This may include but is not limited to: core processing; information and transaction processing and settlement activities that support banking functions such as lending, deposit-taking, funds transfer, fiduciary, or trading activities; Internet related services; security monitoring; systems development and maintenance; aggregation services; digital certification services, and call centers.

[3] The federal banking agencies have authority to regulate and examine services provided to insured depository institutions under 12 U.S.C. 1867(c), 12 U.S.C. 1786(a), and 12 U.S.C. 1464(d)(7).

Outsourcing of information and transaction processing and settlement activities involves risks that are similar to the risks that arise when these functions are performed internally. Risks include threats to security, availability and integrity of systems and resources, confidentiality of information, and regulatory compliance. In addition, the nature of the service provided, such as bill payment, funds transfer, or emerging electronic services, may result in entities performing transactions on behalf of the institution, such as collection or disbursement of funds, that can increase the levels of credit, liquidity, transaction, and reputation risks.[4]

Management should consider additional risk management controls when services involve the use of the Internet. The broad geographic reach, ease of access, and anonymity of the Internet require close attention to maintaining secure systems, intrusion detection and reporting systems, and customer authentication, verification, and authorization. Institutions should also understand that the potential risks introduced are a function of a system's structure, design and controls and not necessarily the volume of activity.

An outsourcing risk assessment should consider the following:

- Strategic goals, objectives, and business needs of the financial institution.
- Ability to evaluate and oversee outsourcing relationships.
- Importance and criticality of the services to the financial institution.
- Defined requirements for the outsourced activity.
- Necessary controls and reporting processes.
- Contractual obligations and requirements for the service provider.
- Contingency plans, including availability of alternative service providers, costs and resources required to switch service providers.
- Ongoing assessment of outsourcing arrangements to evaluate consistency with strategic objectives and service provider performance.
- Regulatory requirements and guidance for the business lines affected and technologies used.

Due Diligence in Selecting a Service Provider

Once the institution has completed the risk assessment, management should evaluate service providers to determine their ability, both operationally and financially, to meet the institution's needs. Management should convey the institution's needs, objectives, and necessary controls to the potential service provider. Management also should discuss provisions that the contract should contain. The appendix to this statement contains some specific factors for management to consider in selecting a service provider.

Contract Issues

Contracts between the institution and service provider should take into account business requirements and key risk factors identified during the risk assessment and due diligence phases. Contracts should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality, and reporting. Management should consider

[4] For example, emerging electronic services may include aggregation. Aggregation is a service that gathers on-line account information from many web sites and presents that information in a consolidated format to the customer.

whether the contract is flexible enough to allow for changes in technology and the financial institution's operations. Appropriate legal counsel should review contracts prior to signing.

Institutions may encounter situations where service providers cannot or will not agree to terms that the institution requests to manage the risk effectively. Under these circumstances, institutions should either not contract with that provider or supplement the service provider's commitments with additional risk mitigation controls. The appendix to this statement contains some specific considerations for management in contracting with a service provider.

Service Provider Oversight

Institutions should implement an oversight program to monitor each service provider's controls, condition, and performance. Responsibility for the administration of the service provider relationship should be assigned to personnel with appropriate expertise to monitor and manage the relationship**.** The number of personnel, functional responsibilities, and the amount of time devoted to oversight activities will depend, in part, on the scope and complexity of the services outsourced. Institutions should document the administration of the service provider relationship. Documenting the process is important for contract negotiations, termination issues, and contingency planning. The appendix to this statement contains some specific factors to consider regarding oversight of the service provider.

Summary

The board of directors and management are responsible for ensuring adequate risk mitigation practices are in place for effective oversight and management of outsourcing relationships. Financial institutions should incorporate an outsourcing risk management process that includes a risk assessment to identify the institution's needs and requirements; proper due diligence to identify and select a provider; written contracts that clearly outline duties, obligations and responsibilities of the parties involved; and ongoing oversight of outsourcing technology services.

APPENDIX

Risk Management of Outsourced Technology Services

Due Diligence in Selecting a Service Provider

Some of the factors that institutions should consider when performing due diligence in selecting a service provider are categorized and listed below. Institutions should review the service provider's due diligence process for any of its significant supporting agents (i.e., subcontractors, support vendors, and other parties). Depending on the services being outsourced and the level of in-house expertise, institutions should consider whether to hire or consult with qualified independent sources. These sources include consultants, user groups, and trade associations that are familiar with products and services offered by third parties. Ultimately, the depth of due diligence will vary depending on the scope and importance of the outsourced services as well as the risk to the institution from these services.

Technical and Industry Expertise

- Assess the service provider's experience and ability to provide the necessary services and supporting technology for current and anticipated needs.
- Identify areas where the institution would have to supplement the service provider's expertise to fully manage risk.
- Evaluate the service provider's use of third parties or partners that would be used to support the outsourced operations.
- Evaluate the experience of the service provider in providing services in the anticipated operating environment.
- Consider whether additional systems, data conversions, and work are necessary.
- Evaluate the service provider's ability to respond to service disruptions.
- Contact references and user groups to learn about the service provider's reputation and performance.
- Evaluate key service provider personnel that would be assigned to support the institution.
- Perform on-site visits, where necessary, to better understand how the service provider operates and supports its services.

Operations and Controls

- Determine adequacy of the service provider's standards, policies and procedures relating to internal controls, facilities management (e.g., access requirements, sharing of facilities, etc.), security (e.g., systems, data, equipment, etc.), privacy protections, maintenance of records, business resumption contingency planning, systems development and maintenance, and employee background checks.
- Determine if the service provider provides sufficient security precautions, including, when appropriate, firewalls, encryption, and customer identity authentication, to protect institution resources as well as detect and respond to intrusions.
- Review audit reports of the service provider to determine whether the audit scope, internal controls, and security safeguards are adequate.

- Evaluate whether the institution will have complete and timely access to its information maintained by the provider.
- Evaluate the service provider's knowledge of regulations that are relevant to the services they are providing. (e.g., Regulation E, privacy and other consumer protection regulations, Bank Secrecy Act, etc.).
- Assess the adequacy of the service provider's insurance coverage including fidelity, fire, liability, data losses from errors and omissions, and protection of documents in transit.

Financial Condition

- Analyze the service provider's most recent audited financial statements and annual report as well as other indicators (e.g., publicly traded bond ratings), if available.
- Consider factors such as how long the service provider has been in business and the service provider's market share for a given service and how it has fluctuated.
- Consider the significance of the institution's proposed contract on the service provider's financial condition.
- Evaluate technological expenditures. Is the service provider's level of investment in technology consistent with supporting the institution's activities? Does the service provider have the financial resources to invest in and support the required technology?

Contract Issues

Some considerations for contracting with service providers are discussed below. This listing is not all-inclusive and the institution may need to evaluate other considerations based on its unique circumstances. The level of detail and relative importance of contract provisions varies with the scope and risks of the services outsourced.

Scope of Service

The contract should clearly describe the rights and responsibilities of parties to the contract. Considerations include:

- Timeframes and activities for implementation and assignment of responsibility. Implementation provisions should take into consideration other existing systems or inter-related systems to be developed by different service providers (e.g., an Internet banking system being integrated with existing core applications or systems customization).
- Services to be performed by the service provider including duties such as software support and maintenance, training of employees or customer service.
- Obligations of the financial institution.
- The contracting parties' rights in modifying existing services performed under the contract.
- Guidelines for adding new or different services and for contract re-negotiation.

Performance Standards

Institutions should generally include performance standards defining minimum service level requirements and remedies for failure to meet standards in the contract. For example, common service level metrics include percent system uptime, deadlines for completing batch processing, or number of processing errors. Industry standards for service levels may provide a reference point. The institution should periodically review overall performance standards to ensure consistency with its goals and objectives.

Security and Confidentiality

The contract should address the service provider's responsibility for security and confidentiality of the institution's resources (e.g., information, hardware). The agreement should prohibit the service provider and its agents from using or disclosing the institution's information, except as necessary to or consistent with providing the contracted services, to protect against unauthorized use (e.g., disclosure of information to institution competitors). If the service provider receives nonpublic personal information regarding the institution's customers, the institution should notify the service provider to assess the applicability of the privacy regulations. Institutions should require the service provider to fully disclose breaches in security resulting in unauthorized intrusions into the service provider that may materially affect the institution or its customers. The service provider should report to the institution when material intrusions occur, the effect on the institution, and corrective action to respond to the intrusion.

Controls

Consideration should be given to contract provisions addressing control over operations such as:

- Internal controls to be maintained by the service provider.
- Compliance with applicable regulatory requirements.
- Records to be maintained by the service provider.
- Access to the records by the institution.
- Notification by the service provider to the institution and the institution's approval rights regarding material changes to services, systems, controls, key project personnel allocated to the institution, and new service locations.
- Setting and monitoring of parameters relating to any financial functions, such as payments processing and any extensions of credit on behalf of the institution.
- Insurance coverage to be maintained by the service provider.

Audit

The institution should generally include in the contract the types of audit reports the institution is entitled to receive (e.g., financial, internal control and security reviews). The contract can specify audit frequency, cost to the institution associated with the audits if any, as well as the rights of the institution and its agencies to obtain the results of the audits in a timely manner. The contract may also specify rights to obtain documentation regarding the resolution of audit disclosed deficiencies and inspect the processing facilities and operating practices of the service provider. Management should consider, based upon the risk assessment phase, the degree to which independent internal audits completed by service provider audit staff can be used and the need for external audits and reviews (e.g., SAS 70 Type I and II reviews).[5]

For services involving access to open networks, such as Internet-related services, special attention should be paid to security. The institution may wish to include contract terms requiring periodic audits to be performed by an independent party with sufficient expertise. These audits may include penetration testing, intrusion detection, and firewall configuration. The institution should receive sufficiently detailed reports on the findings of these ongoing audits to adequately assess security without compromising the service provider's security. It can be beneficial to both the service provider and the institution to contract for such ongoing tests on a coordinated basis

[5] AICPA Statement of Auditing Standards 70 "Reports of Processing of Transactions by Service Organizations," known as SAS 70 Reports, are one commonly used form of external review. Type I SAS 70 reports review the service provider's policies and procedures. Type II SAS 70 reports provide tests of actual controls against policies and procedures.

given the number of institutions that may contract with the service provider and the importance of the test results to the institution.

Reports

Contractual terms should discuss the frequency and type of reports the institution will receive (e.g., performance reports, control audits, financial statements, security, and business resumption testing reports). Guidelines and fees for obtaining custom reports should also be discussed.

Business Resumption and Contingency Plans

The contract should address the service provider's responsibility for backup and record protection, including equipment, program and data files, and maintenance of disaster recovery and contingency plans. Responsibilities should include testing of the plans and providing results to the institution. The institution should consider interdependencies among service providers when determining business resumption testing requirements. The service provider should provide the institution with operating procedures the service provider and institution are to implement in the event business resumption contingency plans are implemented. Contracts should include specific provisions for business recovery timeframes that meet the institution's business requirements. The institution should ensure that the contract does not contain any provisions that would excuse the service provider from implementing its contingency plans.

Sub-contracting and Multiple Service Provider Relationships

Some service providers may contract with third-parties in providing services to the financial institution. To provide accountability, it may be beneficial for the financial institution to seek an agreement with and designate a primary contracting service provider. The institution may want to consider including a provision specifying that the contracting service provider is responsible for the service provided to the institution regardless of which entity is actually conducting the operations. The institution may also want to consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.

Cost

The contract should fully describe fees and calculations for base services, including any development, conversion, and recurring services, as well as any charges based upon volume of activity and for special requests. Cost and responsibility for purchase and maintenance of hardware and software may also need to be addressed. Any conditions under which the cost structure may be changed should be addressed in detail including limits on any cost increases.

Ownership and License

The contract should address ownership and allowable use by the service provider of the institution's data, equipment/hardware, system documentation, system and application software, and other intellectual property rights. Other intellectual property rights may include the institution's name and logo; its trademark or copyrighted material; domain names; web sites designs; and other work products developed by the service provider for the institution. The contract should not contain unnecessary limitations on the return of items owned by the institution. Institutions that purchase software should consider establishing escrow agreements. These escrow agreements may provide for the following: institution access to source programs under certain conditions (e.g., insolvency of the vendor), documentation of programming and systems, and verification of updated source code.

Duration

Institutions should consider the type of technology and current state of the industry when negotiating the appropriate length of the contract and its renewal periods. While there can be benefits to long-term technology contracts, certain technologies may be subject to rapid change and a shorter-term contract may prove beneficial. Similarly, institutions should consider the appropriate length of time required to notify the service provider of the institutions' intent not to renew the contract prior to expiration. Institutions should consider coordinating the expiration dates of contracts for inter-related services (e.g., web site, telecommunications, programming, network support) so that they coincide, where practical. Such coordination can minimize the risk of terminating a contract early and incurring penalties as a result of necessary termination of another related service contract.

Dispute Resolution

The institution should consider including in the contract a provision for a dispute resolution process that attempts to resolve problems in an expeditious manner as well as provide for continuation of services during the dispute resolution period.

Indemnification

Indemnification provisions generally require the financial institution to hold the service provider harmless from liability for the negligence of the institution, and vice versa. These provisions should be reviewed to reduce the likelihood of potential situations in which the institution may be liable for claims arising as a result of the negligence of the service provider.

Limitation of Liability

Some service provider standard contracts may contain clauses limiting the amount of liability that can be incurred by the service provider. If the institution is considering such a contract, consideration should be given to whether the damage limitation bears an adequate relationship to the amount of loss the financial institution might reasonably experience as a result of the service provider's failure to perform its obligations.

Termination

The extent and flexibility of termination rights sought can vary depending upon the service. Contracts for technologies subject to rapid change, for example, may benefit from greater flexibility in termination rights. Termination rights may be sought for a variety of conditions including change in control (e.g., acquisitions and mergers), convenience, substantial increase in cost, repeated failure to meet service levels, failure to provide critical services, bankruptcy, company closure, and insolvency.

Institution management should consider whether or not the contract permits the institution to terminate the contract in a timely manner and without prohibitive expense (e.g., reasonableness of cost or penalty provisions). The contract should state termination and notification requirements with time frames to allow the orderly conversion to another provider. The contract must provide for return of the institution's data, as well as other institution resources, in a timely manner and in machine readable format. Any costs associated with transition assistance should be clearly stated.

Assignment

The institution should consider contract provisions that prohibit assignment of the contract to a third party without the institution's consent, including changes to subcontractors.

Oversight of Service Provider

Some of the oversight activities management should consider in administering the service provider relationship are categorized and listed below. The degree of oversight activities will vary depending upon the nature of the services outsourced. Institutions should consider the extent to which the service provider conducts similar oversight activities for any of its significant supporting agents (i.e., subcontractors, support vendors, and other parties) and the extent to which the institution may need to perform oversight activities on the service provider's significant supporting agents.

Monitor Financial Condition and Operations

- Evaluate the service provider's financial condition periodically.
- Ensure that the service provider's financial obligations to subcontractors are being met in a timely manner.
- Review audit reports (e.g., SAS 70 reviews, security reviews) as well as regulatory examination reports if available, and evaluate the adequacy of the service providers' systems and controls including resource availability, security, integrity, and confidentiality.[6]
- Follow up on any deficiencies noted in the audits and reviews of the service provider.
- Periodically review the service provider's policies relating to internal controls, security, systems development and maintenance, and back up and contingency planning to ensure they meet the institution's minimum guidelines, contract requirements, and are consistent with the current market and technological environment.
- Review access control reports for suspicious activity.
- Monitor changes in key service provider project personnel allocated to the institution.
- Review and monitor the service provider's insurance policies for effective coverage.
- Perform on-site inspections in conjunction with some of the reviews performed above, where practicable and necessary.
- Sponsor coordinated audits and reviews with other client institutions.

Assess Quality of Service and Support

- Regularly review reports documenting the service provider's performance. Determine if the reports are accurate and allow for a meaningful assessment of the service provider's performance.
- Document and follow up on any problem in service in a timely manner. Assess service provider plans to enhance service levels.
- Review system update procedures to ensure appropriate change controls are in effect, and ensure authorization is established for significant system changes.
- Evaluate the provider's ability to support and enhance the institution's strategic direction including anticipated business development goals and objectives, service delivery requirements, and technology initiatives.
- Determine adequacy of training provided to financial institution employees.
- Review customer complaints on the products and services provided by the service provider.
- Periodically meet with contract parties to discuss performance and operational issues.

[6] Some services provided to insured depository institutions by service providers are examined by the FFIEC member agencies. Regulatory examination reports, which are only available to clients/customers of the service provider, may contain information regarding a service provider's operations. However, regulatory reports are not a substitute for a financial institution's due diligence in oversight of the service provider.

- Participate in user groups and other forums.

Monitor Contract Compliance and Revision Needs

- Review invoices to assure proper charges for services rendered, the appropriateness of rate changes and new service charges.
- Periodically, review the service provider's performance relative to service level agreements, determine whether other contractual terms and conditions are being met, and whether any revisions to service level expectations or other terms are needed given changes in the institution's needs and technological developments.
- Maintain documents and records regarding contract compliance, revision and dispute resolution.

Maintain Business Resumption Contingency Plans

- Review the service provider's business resumption contingency plans to ensure that any services considered mission critical for the institution can be restored within an acceptable timeframe.
- Review the service provider's program for contingency plan testing. For many critical services, annual or more frequent tests of the contingency plan are typical.
- Ensure service provider interdependencies are considered for mission critical services and applications.