

BANK TECHNOLOGY BULLETIN ON OUTSOURCING

FIL-50-2001
June 4, 2001

TO:
CHIEF EXECUTIVE OFFICER
SUBJECT:
Bank Technology Bulletin

The attached FDIC Bank Technology Bulletin introduces three short documents containing practical ideas for banks to consider when they engage in technology outsourcing. They are for informational purposes only and should not be considered examination procedures or official guidance.

For further information, please contact DOS E-Banking Branch by e-mail at e-banking@fdic.gov.

Christie A. Sciacca

Director, Bank Technology Group

Attachment: Bank Technology Bulletin

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).



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.

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 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 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.
- 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.
- 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.

¹The 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.

²Technology 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.

³The 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).

⁴For 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.

⁵AICPA 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.

⁶Some 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.



June 4, 2001

Federal Deposit Insurance Corporation

Bank Technology Bulletin

TO: Chief Executive Officers of All FDIC-Supervised Banks

SUBJECT: Technology Outsourcing Information Documents

On November 29, 2000, the FDIC, along with the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration, issued guidance on risk management of technology outsourcing (Financial Institution Letter 81-2000, Risk Management of Technology Outsourcing). The guidance focused on four key areas: risk assessment, service provider selection, contract terms, and oversight of outsourcing arrangements. Because community banks may face particular challenges in engaging and supervising their technology providers, the FDIC has talked with bankers and other experts to identify areas where assistance might be useful. Three informational documents were produced as a result of those discussions:

- Effective Practices for Selecting a Service Provider
- Tools to Manage Technology Providers' Performance Risk: Service Level Agreements
- Techniques for Managing Multiple Service Providers

The documents are being offered as a resource of practical information to community banks on how to select service providers, draft contract terms, and oversee multiple service providers when outsourcing for technology products and services. They have been prepared not as examination procedures or official guidance but as informational tools for community bankers. The documents help answer questions bankers might have about identifying and selecting the best service provider for a task, ensuring that the bank receives the desired level of service, and overseeing outsourced operations that are distributed among multiple service providers.

An additional Bank Technology Bulletin--*Protecting Internet Domain Names*--is posted on the FDIC's Web site at <http://www.fdic.gov/news/news/financial/2000/fil0077a.html>

Printed copies of the documents, which are in the form of brochures, can also be obtained after June 11, 2001, by contacting the FDIC's Public Information Center. Faxed requests are preferred.

Write to:

FDIC Public Information Center 801 17th Street, NW, Room 100, Washington, DC 20434

Fax:

202-416-2076

Telephone:

800-276-6003 or 202-416-6940

For further information, please contact DOS E-Banking Branch by e-mail at e-banking@fdic.gov.

Christie A. Sciacca

Director, Bank Technology Group

Distribution: FDIC-Supervised Banks (Commercial and Savings)

Effective Practices for Selecting a Service Provider

This document is intended to serve as a resource for banks in addressing specific challenges relating to technology outsourcing. The content was prepared not as examination procedures or official guidance but as an informational tool for community bankers.

Introduction

As community banks become more involved in technology outsourcing, they face significant challenges in managing the risks associated with reliance on third party technology service providers¹. Outsourcing has become more complex with many banks using vendors for key business functions and relying on multiple providers.

This brochure suggests techniques that can facilitate the process by which financial institutions conduct due diligence and select the best service provider.



Objectives of the Selection Process

The objective of the selection process is simple: identify the best-qualified service provider and negotiate a contract that meets the needs of the financial institution. The selection process also should be cost effective, efficient, and appropriate for the nature of activities that the bank is seeking to outsource. Of course, the processes that the bank uses to select a provider or team of providers will depend on the criticality and complexity of the service to be outsourced. In addition, the degree of process formality may depend on the nature of the outsourced service and the bank's familiarity with the prospective providers. Also, banks may wish to consider using consultants to provide expertise and assistance throughout the selection process.

Identification of Qualified Providers

Prior to identifying prospective service providers, it is essential that bank management have a clear understanding of the requirements and expectations that they are seeking to meet. As discussed in the FFIEC Guidance, "Risk Management of Outsourced Technology Services," a comprehensive risk assessment should consider how the outsourcing arrangement will support the institution's objectives and strategic plans and how the relationship with the service provider will be managed. The next step in the process involves conducting due diligence to evaluate service providers and determine their ability, both operationally and financially, to meet the institution's needs.

In some situations, the bank will either already know or quickly be able to determine a "short list" of provider candidates. This may occur when a specialized service is offered by a small number of providers, when size or geographic location is important, or when existing relationships with other providers (e.g., the bank's core data processor) are critical factors. If the bank has already identified possible providers and does not seek to expand the pool of candidates, management can proceed to evaluation and contract negotiation.

However, when the bank seeks to create or expand a list of possible service providers, it may be helpful to use tools and techniques such as Requests for Proposal (RFP), Requests for Information (RFI), and Requests for Quote (RFQ). These are ways to obtain specific information about a service provider's ability to meet the bank's requirements and the fees that they charge for the service. In an RFP, the bank outlines its business objectives and technical requirements and solicits responses from service providers that describe their ability to meet these needs and related prices. A more detailed discussion of the RFP process is provided in the Appendix. The RFI and RFQ are respectively targeted at obtaining specific information about the technical solutions that are available and prices charged for a particular service.

In initial communications with service provider candidates, the bank should want to make clear that: (1) the service provider cannot disclose any information about the bank's systems or its business plans to others outside the candidate's team; (2) the service provider expects that commitments made during the selection process will be binding in any final agreement; and (3) the service provider identify all subcontractors, consultants, or third parties on which it is relying to provide services to the bank.

Evaluation and Selection

Once the bank has identified a prospective provider or list of candidates, the evaluation and selection process can commence. Even in situations where only one provider is identified, it is important that the institution still evaluate their technical expertise, operating controls, financial condition, and management. When a larger group of candidates is being considered, the evaluations can be quantified and ranked to facilitate selection of a small number of the best-qualified providers.

The evaluation criteria are essential to the selection process and allow the financial institution to methodically review the candidates' proposals. The overriding objective is to select the most qualified provider. Utilizing standard evaluation criteria assists in this selection effort. Some suggested evaluation criteria are:

- Compatibility of the service provider's vision/value proposition with that of the bank.
- Ability to execute the vision/value proposition.
- Functionality of the service or system proposed. (Do the functional features meet the stated requirements?)
- Technology in terms of type, power, modularity, and ability to upgrade/refresh or scale.
- Service and support in terms of maintenance hours, response time, resolution time, security, disaster planning, and other service levels.
- Cost/Price.
- Financial stability of the vendor.

Depending on the situation and the outsourced activity, each of the above criteria may be given greater or less weight in the overall evaluation. Other criteria may be considered, as appropriate. In addition, bank management may consider on-site visits, reference checks, and inquiries with industry groups and peer institutions.

The following represent suggested practices that can facilitate the evaluation process:

- Be specific in all requests for information from candidates. Prioritize the requested information and indicate minimums and maximums for the length of response. A useful rule of thumb is that "You get what you ask for."
- Consider using numerical scores based on quality ranking factors. By using consistent scoring systems or metrics, objective evaluation standards can be applied. Make sure the quality ranking factors are aimed at achieving the bank's goal.
- Determine minimum acceptable scores for the criteria used before rating the bids. Narrow the list of proposals by eliminating bids that do not meet the required minimums.
- Document the evaluation process and methodology used to score the respective proposals. It is generally a good practice to document requirements and priorities before starting the evaluation stage of a project.
- Consider conducting meetings and/or oral presentations where service providers can respond to questions and provide additional information.
- Consider ways to keep the process manageable. Depending on the complexity of the outsourced activity, the evaluation process can be time consuming and resource intensive.
- When working with a larger list of prospective candidates, narrow the group to a small number (e.g., two or three) to solicit "best and final" offers.

Negotiating the Contract

Communication with prospective providers can commence at various points in the evaluation and selection processes. For example, clarifications or requests for additional information may be needed to fully evaluate a proposal. Meetings and oral presentations may be useful to engage the provider in more detailed discussions. Informational meetings may also be useful to determine a provider's willingness to depart from their original proposal in terms of price or services offered. Banks may also choose to engage multiple candidates in discussions concurrently to compare their responses.

After the selection process has narrowed the choice to one or a small number of strong candidates, negotiations with the provider(s) can help the bank finalize the terms of the contract. The negotiation process can help the bank establish terms that are agreeable to all parties and confirm that there is common understanding of the roles and responsibilities. Direct communication with the provider may help to determine whether organizational cultures are compatible and may provide an opportunity to interact with personnel who will play a key role in the future relationship.

Negotiating a contract is the final step in the procurement process. If a Request for Proposal was used or a Statement of Work was provided to the candidates to solicit their proposals, these documents can be directly incorporated into the contract. Key terms and conditions, as well as technical solutions and pricing, are generally established based on the proposal responses and final offers. A few points that might be useful in the contract negotiation and approval phases follow:

- As a general industry practice, information technology contracts are commonly set for a three- to five-year term. The shorter term enables the institution to reflect the pace of change in the technology industry.
- Prices indicated in the contract and service provider's proposal can be more effectively considered when they are broken down by each category of service (workspace, network services, etc.) and for the technology services by platform group.
- It is useful to explicitly state all charges as part of the invoicing procedures, occupancy policy, communication protocols, additional test time, and annual increases. Specifying each additional increment of cost is important in order to minimize the financial risk of increased prices for additional or reduced workload.
- Many contracts contain exit clauses that allow the institution to cancel the contract for reasons such as a failure to perform.
- Service level agreements should be stated in the contract. (Further information on service level agreements is provided in a separate FDIC document on technology outsourcing.)
- Having a clear understanding of the current and anticipated future requirements of the outsourced service can allow the bank to obtain a long-term solution rather than a quick fix.
- Set a realistic time line for completing the contract negotiation process.
- Obtain a list of all key personnel and a list of any subcontractors, consultants, or third parties on which service delivery depends.

Summary

Selection of a competent and qualified service provider is perhaps the most critical part of the outsourcing process. The process of selecting a vendor and determining their qualifications may vary in its formality and requirements for time and resources. Key determinants of the process will be the bank's foreknowledge of qualified providers and the number of candidates under consideration. Criteria for selection should be determined in advance to facilitate the evaluation process. Once a single or handful of qualified providers has been identified, further negotiations can help to finalize an agreement that is mutually beneficial.

The final outcome of the process should be the selection of a viable service provider that meets the procurement needs and objectives of the bank. Undertaking this commitment can provide significant benefits for complex information technology services or projects. Benefits include, but

are not limited to, focusing the bank on the objective and strategic fit of the procurement, as well as facilitating due diligence in the selection of a service provider.

APPENDIX

Requests for Proposal (RFP) - Definition and Overview

A Request for Proposal is a tool that can be used to facilitate the selection of a qualified service provider and assist with the contracting process. The RFP can help a financial institution identify the best service provider(s) for their specific requirements by inviting competition, as service providers respond with a solution or combination of solutions, and the institution selects the most viable provider. The RFP can be particularly useful when bank management is seeking to create or expand a list of potential service providers or when projects are complex and represent a strategic or long-term enterprise investment.

The Process

The RFP process consists of a set of tasks that can be grouped into three major categories: development of a baseline, proposal preparation, and selection activities. The following are some of the many tasks that are generally part of the RFP and vendor selection process. The list is not intended to be all-inclusive, and the steps may either be expanded or contracted to meet the needs of any particular situation.

Development of a Baseline:

- Determine the purpose and goal of the procurement.
- Assign a proposal project team and an evaluation team.
- Plan the outsourcing project in terms of cost schedule, functional requirements, and resource requirements.
- Develop a "baseline" that represents a current "as is" description of the affected environment in terms of current cost, inventory of systems, and services.
- Develop a "needs assessment" which describes management's assumptions on how to more effectively serve its customers.
- Determine the future requirements by analyzing anticipated needs and project objectives.
- Determine the disparity between the current environment and the future requirements in order to identify the gaps that need to be filled to get from the current environment to the desired environment.

The various tasks that comprise the baseline activity are designed to establish a clear picture of the goal and objective of the procurement. In addition, a detailed understanding of the current environment is typically established in order to determine if there is a gap between the current environment and future needs. Finally, this baseline understanding of cost and service levels is useful in conducting a cost/benefit or return on investment analysis.

Proposal Preparation:

- Develop the Statement of Work, a technical document that outlines basic requirements.
- Draft the RFP based on the contents of the Statement of Work.

Proposal preparation tasks are focused on defining the requirements, which are then presented in the form of a Statement of Work or similar document. The Statement of Work indicates desired services, the roles and responsibilities of each party, and the required service levels or performance standards.

A Typical RFP Format Includes the Following:

- Executive summary.
- Introduction:
 - Background on the financial institution and/or business division
 - Scope of services being requested, (e.g., web hosting, infrastructure outsourcing, disaster recovery, etc.).

- Background on the business process, including current status, existing roles, and responsibilities of the people who will be working with the vendor.
 - Statement on the confidentiality of information.
- Overview:
 - Statement of mission/vision of the financial institution.
 - Statement of business objectives the institution wants to achieve.
 - Statement of scope in terms of which business functions, business units, applications, packages, geographies, and technology platforms are being covered by the RFP.
 - Role of the service provider.
- Project schedule:
 - Service provider RFP question deadline.
 - Service provider analysis meeting (optional).
 - Proposal due date. (Generally, according to industry practices, service providers need four weeks to respond comprehensively to anything other than simple configurations. Less time may result in poorer, less innovative and probably costlier solutions.)
 - Service provider demonstration day.
 - Contract negotiation.
 - Final decision.
 - Proposed implementation start date.
- Statement of Work:
 - Detailed technical requirements, describing the required business applications and their functionality, as well as the hardware and infrastructure platform and communications requirements for each outsourced area and operational configuration.
 - Transition, implementation, training, start-up, maintenance, and security requirements.
 - Performance criteria for success of solution.
 - Project management and service level reporting requirements.
 - Indication of performance/service level incentives and penalties.

Tools to Manage Technology Providers' Performance Risk: Service Level Agreements

This document is intended to serve as a resource for banks in addressing specific challenges relating to technology outsourcing. The content was prepared not as examination procedures or official guidance but as an informational tool for community bankers.

Introduction

As community banks outsource more of their mission critical applications, properly managing the relationships between financial institutions and technology service providers¹ becomes increasingly important. This brochure discusses the Service Level Agreement (SLA) as an effective tool for managing the risks associated with technology outsourcing and describes practices for measuring and monitoring service providers' performance.

What Are Service Level Agreements?

Service Level Agreements (SLAs) are contractually binding clauses documenting the performance standard and service quality agreed to by the bank and service provider. The SLA is a key component in structuring a successful outsourcing contract. The SLA ensures that the institution receives the services it wants at the expected performance standard and price. As such, the SLA is a key component in managing the financial and operational risk involved with outsourcing contracts. It also can be one way to help mitigate risk. By specifying the measurement unit and service range for the selected category, the risk of poor service may be diminished because it becomes an area of focus and is designated as the service provider's responsibility.



The SLA's primary purpose is to specify and clarify performance expectations, as well as establish accountability. Therefore, balancing the need for precise measurement standards with sufficient flexibility is important. A common pitfall is excessive oversight or "micro-management" of the provider responsible for the service, which can also burden the bank employees charged with supervising the service provider relationship and monitoring the SLAs.

A well-designed SLA will recognize and reward, or at least acknowledge, good service. It will also provide the measurement structure -- or performance metric -- to identify substandard service and trigger correction or cancellation provisions as warranted. In today's outsourcing environment, incentives or penalties in the SLA can be an effective tool for managing service. If services received do not measure up to expectations, direct consequences, such as reduced levels of compensation or a credit on future services, would result.

Structuring and Developing SLAs

A typical SLA includes the following components and is tailored to fit the nature of the outsourced service or application:

- Service category (e.g., system availability or response time).
- Acceptable range of service quality.
- Definition of what is being measured.
- Formula for calculating the measurement.
- Relevant credits/penalties for achieving/failing performance targets.
- Frequency and interval of measurement.

Before an SLA is signed, the service provider and the institution should clarify and establish expectations. Unless these expectations are clearly measurable, the service category will be difficult to manage due to the bank's and the vendor's differing goals and perspectives.

Developing a Successful SLA Involves Four Steps

- Determining objectives - Reviewing the strategic business needs of the financial institution includes evaluating its day-to-day operating environment, risk factors, and market conditions. Consideration should be given to how the outsourced service fits into the bank's overall strategic plan.
- Defining requirements - Identifying the operational objectives (e.g., the need to improve operating efficiency, reduce costs, or enhance security) will help the institution to define performance requirements. It will also help identify the levels of service the bank needs from the service provider to meet its strategic goals and objectives for the outsourced activity.
- Setting measurements - Clear and impartial measurements – or metrics - can be developed once the strategic needs and operating objectives have been defined. The metrics are used to measure and confirm that the necessary service levels have been achieved and the objectives and strategic intent have been met.
- Establishing accountability - It is useful to develop and adopt a framework that ensures accountability after the measurement units (i.e., the metrics) have been clearly defined. The service provider rarely owns accountability and responsibility for all tasks. Establishing this accountability usually includes a clear statement of the outcome if the level of service is exceeded or if the expected service fails to meet the stated standard.

The SLA development process and each of the four steps are discussed in further detail in Appendix 1. A sample SLA is provided in Appendix 2.

Representatives from the institution (management, legal counsel, and information technology staff) and the service provider typically meet to ensure that performance metrics and targets are properly addressed when developing SLAs. Bank management may also consider interviewing some of the system users to help identify important criteria to incorporate into the SLAs. Reaching agreement on specific SLAs may involve significant discussion and negotiation between the bank and the service provider. The bank may wish to consult with peer institutions and trade associations about useful benchmarks for performance standards. This information may be helpful in the contract negotiation process and assist the bank in determining if the service levels offered by the provider are reasonable and standard.

Drafting Successful Service Level Agreements

Sufficient time and resources should be devoted to preparing SLAs. The agreement will be the primary document governing the procurer and vendor of services that may have a significant impact on the bank's performance. The following items are important reminders for institutions drafting SLAs and selecting the metric(s) to be used to measure vendor performance:

- Focus on the most important areas. Financial institutions should identify the performance and risk factors that are most crucial to the success of the outsourced function. The institution should invest its time drafting strong SLAs for these areas. Areas with minimal effect on the process will be of less importance and, accordingly, should have less prominence in the contracting process.
- Make sure that performance metrics measure what the bank wants them to measure. Verify that the metrics used to govern the SLA appropriately represent the functions that the bank intends to measure.
- The metrics should measure the performance the service provider is giving the bank, and not be based on the performance the vendor is delivering in aggregate to all its customers.
- Ensure that SLAs are focused on institutional goals. Avoid the trap of creating agreements that are focused on the success of the individual process without regard for

- the how the process addresses a corporate goal. Each measurement should logically support a requirement that is linked to a strategic goal.
- Be specific. Ensure that all parties involved in the SLA understand the terms spelled out in the agreement. Terms should be clearly defined to avoid different interpretations. Spending extra time defining terms when creating an agreement can prevent misunderstandings and loss of time and money caused by differing interpretations of the intent of the SLA.

Managing SLAs

It is worthwhile for the institution to provide for ongoing management of the agreement when a SLA is established. The SLA management process usually goes beyond performance measurement to ensure success. Generally, the measurement process should be kept as simple as possible, emphasizing timely identification of deviations from agreed upon performance metrics. Ongoing communication between the bank and the service provider is also important. The following four-phase methodology is based on observed industry practices that can help banks manage SLAs effectively:

- Measure service activity results against defined service levels.
- Examine measured results to identify problems and determine causes.
- Take appropriate action to correct failed activities, functions, and/or processes.
- Continuously guide service providers through feedback sessions based on objectively measured performance metrics.

Before signing an outsourcing contract, the bank may find it beneficial to verify that important performance requirements have been addressed, risks have been identified, and each service level is defined. Each measurement should be defined clearly and concisely. This will provide the foundation for effectively managing service levels throughout the four phases of the SLA management process.

SLA management is an ongoing process, and is viewed as an integral component of the outsourcing relationship. A suggested practice is to include periodic review and change provisions in the SLA to ensure that service level goals and performance measurements can meet the changing business and technology needs of the institution.

Summary

Service Level Agreements are tools to measure, monitor, and control the operational and financial risks associated with outsourcing technology services. Essential to this process is establishing realistic performance metrics and continuous problem tracking and resolution. The bank should consider working closely with service providers to identify, verify, and correct problems; perform root-cause analysis; and make process modifications to prevent problems from recurring. As the outsourcing relationship progresses, SLAs should reflect the evolution of services provided. Accordingly, they should be updated to facilitate continued service improvement. Well-constructed SLAs are an effective tool for managing service provider performance and ensuring that the bank receives the quality of service that it needs and expects.

APPENDIX 1 – Developing SLAs

Four-Step Process

While many factors determine how the bank and its service provider will agree to manage the quality of service, the four-step process² outlined below may be helpful in developing successful SLAs. This process facilitates identifying essential requirements for the outsourced service and translating the requirements into measurable and accountable performance standards.

- Determining objectives.
- Defining requirements.
- Setting measurements.
- Establishing accountability.

Determining Objectives

The first step in creating an SLA is determining the standards the outsourced activity needs to meet in order to assist the bank in attaining its strategic goals. The bank should consider the criticality of the activity to the bank's mission and weigh the impact success or failure will have on the bank's operations or reputation. The institution also needs to consider the relationship of the outsourced activity to other systems, applications, and functions in the bank and take into account any critical interdependencies. Based on this analysis, the bank can identify the objectives that are critical in ensuring the success of the function. For each activity, function, and process, a clear objective is needed to understand what constitutes success.

Defining Requirements

In order to attain strategic goals, it is important to identify how the institution is going to achieve the objectives that have been set. To establish these requirements, the institution can break the objectives down into specific activities that must be undertaken to achieve the goal. While the objectives refer to broad statements geared toward attaining success, the performance requirements are targeted at the specific activities that the bank can require from the service provider to ensure the strategic objective is met.

Setting Measurements

In formulating an agreement, the bank can identify specific measurements that indicate if the prescribed requirements are being met. The measurements – or metrics - that correspond to the performance requirements represent tangible or quantifiable deliverables that bank management can monitor and discuss with the service provider, as appropriate. Target metrics should be objective and clearly linked to the bank's business needs and risk management requirements. Metrics should be established based on specific tolerance levels and the minimum acceptable levels of service. A minimum acceptable level of service also should be set to define the point of significant failure.

The following table provides two examples of strategic objectives and related performance requirements, along with target metrics. The first objective pertains to system security and may be appropriate for an outsourced activity involving sensitive data or applications. The second objective addresses certain reliability and availability needs that may be associated with an outsourced system that processes or stores information essential for bank employees or customers. The corresponding performance requirements and measurements provide the means to quantify and document service provider performance.

Table 1 - Examples of Objectives, Requirements, and Measurements

Strategic Objective	Performance Requirement	Measurement
	Sensitive system and bank/customer data must be protected with strong security.	Regular checks for intrusions or other security breaches. Copies of intrusion scan reports to be sent at pre-determined frequency.
	Periodic security assessments, tests, or reviews.	Copies of independent security assessment reports to be provided at pre-determined frequency.
	Timely reporting of incidents and follow up to bank management. Regular incident reports (frequency will depend upon system criticality). Mission critical systems must be reliable and available. System downtime must be minimal. Specified requirement for system uptime (e.g., 99.9%).	
	The system must be able to support certain volumes of activity at a given time. Specified requirement or parameters for capacity (e.g., 1,000 transactions processed per minute).	

Establishing Accountability

Clear definitions of accountability are important to ensure that both the bank and the service provider understand their roles and responsibilities for each service level requirement. However, beyond simply designating a role or activity, accountability should also be established by specifying the consequences if a given service level is not met. Incentives and penalties can play a key role in establishing accountability. Incentives can be used to motivate a service provider to meet or exceed specified service levels by offering a reward. Rewards should generally be attractive enough to motivate the provider, but less than the actual financial value provided by the service. Penalty clauses also should be considered and bank management should have the right to exercise these penalties for any defined service delivery failures.

When negotiating incentives and penalties into an SLA, it is helpful to consider:

- The importance of the performance measure to the bank^{3/4} This will help the bank determine how to weight the associated incentives/penalties as well as the frequency for monitoring performance.
- Each party's expectations for quality and consistency^{3/4} These factors, coupled with prior experiences, may help the bank determine the best method for motivating the provider toward desired performance.
- The severity of the consequences to the bank if key performance measures are not met^{3/4} The effect on the institution should be a motivating factor for the institution when determining whether compensation clauses or other remedies should be provided.

APPENDIX 2 – Sample Service Level Agreements

(Note: This SLA is for illustration purposes only, and not to be relied upon as a model contract for any specific service agreement. Actual SLAs will vary widely depending on the services contracted. Additional provisions or an increase in the scope of this SLA will be necessary to govern other aspects of the relationship, such as security. Consult with bank legal counsel for specifics of contract clauses and formation advice.)

Purpose

This agreement is between Buyer and Vendor. This document outlines the service level roles, responsibilities, and objectives of Buyer and Vendor in support of the given functional area.

Scope of Services

Vendor will house, manage, and operate all hardware and software necessary to provide Internet banking applications to Buyer.

Service Category

This SLA addresses application availability.

Acceptable Range of Service Quality

The Internet banking application shall be available at least 99.5% of each week.

Definition of What is Being Measured

"Availability" will be measured as the percentage of minutes each day that the Internet banking application will be able to receive and respond to messages from the Internet. The server's ability to receive messages will be ascertained using time-check availability software.

Formula for Calculating the Measurement

System availability shall be measured as the number of minutes per day that the Buyer's Internet banking application is capable of receiving and responding to messages from the Internet divided by 1,440 (the total number of minutes in a day).

A 30-minute period from 2:00 AM to 2:30 AM shall be excluded from the calculation because Vendor will be performing system maintenance at this time each day.

Relevant Credits/Penalties for Achieving/Failing Performance Targets

If Vendor is unable to provide this service level to Buyer, Vendor will provide priority support to Buyer until performance levels are met. Service below the prescribed level will result in a rebate of 50% of the monthly fee for the month in which the exception takes place.

If Vendor fails to provide the agreed upon service level for more than two consecutive months, Buyer shall have the right to renegotiate the contract and/or terminate this agreement.

Frequency and Interval of Measurement

The system's availability shall be measured daily by Vendor using time-check availability software. Vendor shall submit monitoring reports generated by this program to Buyer on a weekly basis.

Buyer's Responsibilities

Buyer shall review all monitoring reports and advise Vendor of any deviations from this agreement in a timely manner.

(Include any other items that Buyer will need to do so that Vendor may perform its tasks.)

Vendor's Responsibilities

Vendor shall assume responsibility for customer communications at the point that customer messages leave the Internet service provider.

Vendor shall ensure that all messages are processed in a timely fashion. (Be sure to define the specifics of "timely" standards.)

Vendor shall ensure that the system shall be able to accept and respond to 1,200 inquiries per minute.

(Include any other items that Vendor will need to do to provide the prescribed level of service to Buyer.)

Escalation Guidelines

In the event that Vendor is unable to meet the terms of this agreement, the CIO of Buyer and IT Manager of Vendor shall discuss resolution of the situation. If Vendor will be unable to provide service for more than two hours, Vendor's contingency operating plan shall be invoked.

Renegotiations

Authorized representatives of Buyer and Vendor must mutually agree upon changes to this SLA. All changes must be made and agreed to in writing.

Either party may request review of this SLA at any time. Each party will review the SLA annually and advise the other party of any desired changes.

¹Technology 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. Other terms used to describe Service Providers include vendors, subcontractors, external service provider (ESPs) and outsourcers.

² The "Four Steps" for developing SLAs are based, in part, on research from the Gartner Group entitled "Key Factors in SLA Development."

Techniques for Managing Multiple Service Providers

This document is intended to serve as a resource for banks in addressing specific challenges relating to technology outsourcing. The content was prepared not as examination procedures or official guidance but as an informational tool for community bankers.

Introduction

Financial institutions increasingly rely on a wide variety of service providers¹ to support an array of technology-related functions. Outsourcing information technology to multiple service providers may provide banks with a variety of benefits including access to expert technology skills, lower costs, and increased productivity. However, these arrangements also may alter the risk profile of the institution. Specifically, risk management processes involving outsourced activities are often distributed among several companies and may necessitate a coordinated contract oversight approach by bank management.



This brochure discusses two techniques to manage risks inherent in multiple service provider relationships. The first technique involves the use of a lead contractor to manage the bank's various technology providers. The second technique, which may present its own set of implementation challenges, involves the use of operational agreements between each of the service providers.

Multiple Service Provider Relationships

A multiple service provider relationship typically involves an environment where two or more service providers collaborate to deliver an end-to-end solution to the financial institution. Each one of the service providers has their own core competence and focus area. Together, these providers strive to deliver an integrated service and solutions package to the bank. The nature of the contractual relationship between the service providers and the bank often varies from institution to institution. In many cases, institutions use a lead provider who, in turn, subcontracts with other service providers. Direct "stand-alone" contracts between the bank and each of its service providers represent another common approach.

Multiple service provider arrangements are often used in the deployment of an electronic commerce solution. For example, a web-hosting firm may work with a communications carrier and one or more application service providers.² The financial institution may have separate contracts with each provider (carrier, web host, application service provider) or may have one lead entity (such as the application service provider) that then subcontracts with the carrier, web host, and other providers.

Stand-alone contracts with each service provider usually call for increased day-to-day management of each provider. Additionally, if coordination among each provider is not a requirement of the individual agreements, the opportunities for schedule and performance problems and complexities are likely to arise. Contracting for a technology solution by utilizing one lead provider may diminish the need for the bank to become directly involved if subcontractors fail to perform and/or miss their agreed-to schedule. The lead provider will be solely responsible for meeting the contractual obligations of the subcontractors to other service providers and the bank.

Each financial institution will want to consider the most appropriate risk management strategy when contracting for technology services. Assigning a lead contractor and utilizing inter-provider

service level agreements are two techniques that, if deployed correctly, can assist the institution in managing risks related to complex technology outsourcing arrangements.

Using a Lead Contractor

Bank management may select to structure a multiple provider outsourcing arrangement by designating a lead contractor who is responsible for establishing subcontracts with the other providers and managing their performance. This structure may result from a bank's existing relationship with a service provider who subsequently subcontracts with other firms to provide additional applications and features. A lead contractor structure can also result when a group of providers bid on a contract as a team with pre-established roles and relationships.

Regardless of whether the relationship between the lead contractor and the subcontractors was pre-existing, there are techniques that bank management can employ to manage risks associated with dependence on the lead provider. These techniques, which include provisions in the Statement of Work for defining roles and responsibilities of the contracting parties, are detailed further in the Appendix.

An effectively implemented lead contractor relationship ultimately increases the performance risk for the lead provider, even though it simplifies the boundaries of the relationship. This is due to the fact that the lead provider assumes responsibility for all aspects of the contract, and therefore for the performance of all subcontractors. This structure allows the bank to establish a single point of responsibility for the entire relationship. A contract that clearly defines the roles of the lead provider and subcontractors may streamline the negotiations of legal issues such as the limitations of liability, indemnity, and warranty since responsibility need not be divided among multiple parties. It may also enhance the efficiency of the general contracting process.

Many lead contractors may already have existing arrangements with potential subcontractors for the provision of various ancillary services. As a result, there may be a preference for selecting one of the subcontractors with which the contractor already does business. Financial institutions may wish to carefully examine all contractual provisions in their agreements with the lead contractor to determine the level of responsibility the lead contractor is willing to accept for the actions of the subs that the lead contractor selects.

In some cases, the lead contractor may include contract language that attempts to eliminate all responsibility for losses caused by the subcontractors or sets a fixed dollar limit on the lead contractor's maximum liability for any claims regarding the work of the subcontractors. Financial institutions may wish to consult their legal counsel in order to determine potential exposure to losses for which there may be no ready recovery. It is also important to note that, when using a lead contractor, the financial institution lacks direct privity³ of contract with the subcontractors and will have less influence over the specific activities of each subcontractor.

Using Inter-Provider Operating Agreements

Financial institutions that prefer to maintain a direct contractual relationship with a variety of technology service providers can choose to integrate their efforts by negotiating for operational agreements directly with each of their service providers. This operational agreement can take the form of inter-provider Service Level Agreements (SLAs). This type of SLA is a separate contract requiring each of the providers to meet the other providers' service or performance requirements. Examples of such requirements include on-time delivery of a critical application or platform, network or platform availability specifications, and security requirements. This type of agreement requires the individual providers to communicate and work together.

Implementing operating agreements between various service providers can be challenging because the bank may lack significant negotiating leverage. Although some additional leverage may be gained by negotiating through user groups, challenges remain in attempting to deviate

from the standard forms, contract structure, and delivery approach of established providers. Notwithstanding this, it is important to stress that the intent of the inter-provider agreements is to encourage co-operation and communication between technology providers implementing integrated systems and services.

Communication and co-operation begin with the financial institution developing well thought-out contract goals and objectives that have been agreed to by the senior executives, business managers, and information technology managers and clearly articulating these to the service providers. Contract terms and conditions can be established based on these goals. When determining how goals and objectives will be met, it is helpful to clearly define handoff points between the various service providers.

In addition, bank management and legal counsel may consider establishing the minimum acceptable levels of service that are expected of participating providers as their respective contribution to the team. The minimum service levels provide the performance floor for the inter-provider agreements. Any provider that does not meet these minimum performance standards should be held responsible. Therefore, it may be useful to ask that all service providers participate in developing the inter-provider agreements and accept and agree to the specific terms, minimum performance standards, and the corresponding metrics that will be used to measure their individual and collective performance.

Considerations for Financial Institutions

The following points represent suggested practices that can be helpful to banks in administering outsourced arrangements involving multiple service providers.

- Be explicit about where the ultimate responsibilities lie. If there is a lead contractor, try to make that organization responsible for as much of the overall activity as possible. Be certain everyone knows who is responsible for what, even if some of that responsibility ultimately rests with the institution itself.
- Incorporate protection, in the form of contract provisions for renegotiation, re-evaluation, exit strategies, and other similar activities, into the agreement.
- Include contract provisions that spell out the conditions for subcontractor relationships that are beyond the initial participants. Institutions might define the circumstances for which they have explicit approval and who can be selected to fulfill what function.
- Specify the circumstances when new service providers may be brought into the relationship. This can help minimize the tendency of service providers to resist bringing in new parties and avoid situations where such resistance hinders productive working relationships.
- Retain within the organization the capability to monitor and manage the entire relationship effectively, even if the bank relies heavily on the lead provider or a third party vendor for relationship management.
- Ensure that the lead provider and all subcontractors agree to share and make available all contractor-specific and proprietary technology needed for the services provided. If any sub-contractors or even the lead provider are replaced, all proprietary technology and critical applications should be made available to the replacement provider/subcontractor.

Summary

To manage multiple service provider outsourcing relationships successfully, institutions may find it helpful to focus on three issues:

- Adopt an appropriate outsourcing strategy given the particular objectives sought by the bank (e.g., lead-subcontract approach or multiple single contract relationships).
- Use a contract that comprehensively addresses and outlines the roles and responsibilities of all parties involved. The contract should include provisions for

- approving subcontractors as well as defining the expected levels of service to be provided to the bank.
- Ensure that effective communication channels are maintained between all relevant parties.

Ultimately, the key to successful management of a multiple service provider environment is contract oversight. Regularly scheduled reviews can help point out problems early enough to effect resolution before matters get out of control. Institutions may wish to develop guidelines in the contract that define regular interaction between the service provider(s) and bank managers.

¹ 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. Other terms used to describe Service Providers include vendors, subcontractors, external service provider (ESPs) and outsourcers.

² Application Service Providers (ASPs) specialize in providing business applications and processing power to banks.

³ Privity is a legal term defined as "A relation between parties held to be sufficiently close and direct to uphold a legal claim on behalf of or against another party with whom this relation exists." (Webster's II New Riverside University Dictionary)