Federal Financial Institutions Examination Council

FFIEC

Outsourcing Technology Services

OT

JUNE 2004

IT EXAMINATION

HANDBOOK

Table of Contents

Introduction

The financial services industry has changed rapidly and dramatically. Advances in technology enable institutions to provide customers with an array of products, services, and delivery channels. One result of these changes is that financial institutions increasingly rely on external service providers for a variety of technology-related services. Generally, the term "outsourcing" is used to describe these types of arrangements.

The Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) "Outsourcing Technology Services Booklet" (booklet) provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships.

The ability to contract for technology services typically enables an institution to offer its customers enhanced services without the various expenses involved in owning the required technology or maintaining the human capital required to deploy and operate it. In many situations, outsourcing offers the institution a cost effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines that use it. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action remain. Because the functions are performed by an organization outside the financial institution, the risks may be realized in a different manner than if the functions were inside the financial institution resulting in the need for controls designed to monitor such risks.

Financial institutions can outsource many areas of operations, including all or part of any service, process, or system operation. Examples of information technology (IT) operations frequently outsourced by institutions and addressed in this booklet include: the origination, processing, and settlement of payments and financial transactions; information processing related to customer account creation and maintenance; as well as other information and transaction processing activities that support critical banking functions, such as loan processing, deposit processing, fiduciary and trading activities; security monitoring and testing; system development and maintenance; network operations; help desk operations; and call centers. The booklet addresses an institution's responsibility to manage the risks associated with these outsourced IT services.

Management may choose to outsource operations for various reasons. These include:

- Gain operational or financial efficiencies;
- Increase management focus on core business functions;
- Refocus limited internal resources on core functions;
- Obtain specialized expertise;
- Increase availability of services;
- Accelerate delivery of products or services through new delivery channels;

- Increase ability to acquire and support current technology and avoid obsolescence; and
- Conserve capital for other business ventures.

Outsourcing of technology-related services may improve quality, reduce costs, strengthen controls, and achieve any of the objectives listed previously. Ultimately, the decision to outsource should fit into the institution's overall strategic plan and corporate objectives.

Before considering the outsourcing of significant functions, an institution's directors and senior management should ensure such actions are consistent with their strategic plans and should evaluate proposals against well-developed acceptance criteria. The degree of oversight and review of outsourced activities will depend on the criticality of the service, process, or system to the institution's operation.

Financial institutions should have a comprehensive outsourcing risk management process to govern their technology service provider (TSP) relationships. The process should include risk assessment, selection of service providers, contract review, and monitoring of service providers. Outsourced relationships should be subject to the same risk management, security, privacy, and other policies that would be expected if the financial institution were conducting the activities in-house. This booklet primarily focuses on how the bank regulatory agencies review the risk management process employed by a financial institution when considering or executing an outsourcing relationship.

To help ensure financial institutions operate in a safe and sound manner, the services performed by TSPs are subject to regulation and examination. [1] The federal financial regulators have the statutory authority to supervise all of the activities and records of the financial institution whether performed or maintained by the institution or by a third party on or off of the premises of the financial institution. Accordingly, the examination and supervision of a financial institution should not be hindered by a transfer of the institution's records to another organization or by having another organization carry out all or part of the financial institution's functions. [2]

Many of the general principles on effective management of outsourcing relationships discussed in this booklet can and should be applied to managing the outsourcing of software development. Outsourcing of activities related to software development is addressed in the IT Handbook's, "Development and Acquisition Booklet."

This booklet rescinds and replaces Chapter 22 of the 1996 FFIEC Information Systems Examination Handbook, IS Servicing - Provider and Receiver.

Board and Management Responsibilities

Action Summary

The financial institution's board and senior management should establish and

approve risk-based policies to govern the outsourcing process. The policies should recognize the risk to the institution from outsourcing relationships and should be appropriate to the size and complexity of the institution.

The responsibility for properly overseeing outsourced relationships lies with the institution's board of directors and senior management. Although the technology needed to support business objectives is often a critical factor in deciding to outsource, managing such relationships is more than just a technology issue; it is an enterprise-wide corporate management issue. An effective outsourcing oversight program should provide the framework for management to identify, measure, monitor, and control the risks associated with outsourcing. The board and senior management should develop and implement enterprise-wide policies to govern the outsourcing process consistently. These policies should address outsourced relationships from an end-to-end perspective, including establishing servicing requirements and strategies; selecting a provider; negotiating the contract; and monitoring, changing, and discontinuing the outsourced relationship.

Factors institutions should consider include:

- Ensuring each outsourcing relationship supports the institution's overall requirements and strategic plans;
- Ensuring the institution has sufficient expertise to oversee and manage the relationship;
- Evaluating prospective providers based on the scope and criticality of outsourced services;
- Tailoring the enterprise-wide, service provider monitoring program based on initial and ongoing risk assessments of outsourced services; and
- Notifying its primary regulator regarding outsourced relationships, when required by that regulator. [3]

The time and resources devoted to managing outsourcing relationships should be based on the risk the relationship presents to the institution. To illustrate, outsourcing processing of a small credit card portfolio will require a different level of oversight than outsourcing processing of all loan applications. Additionally, smaller and less complex institutions may have less flexibility than larger institutions in negotiating for services that meet their specific needs and in monitoring their service providers.

Risk Management

Risk management is the process of identifying, measuring, monitoring, and managing risk. Risk exists whether the institution maintains information and technology services internally or elects to outsource them. Regardless of which alternative they choose, management is responsible for managing risk in all outsourcing relationships. Accordingly, institutions should establish and maintain an effective risk management process for initiating and overseeing all outsourced operations.

An effective risk management process involves several key factors:

- Establishing senior management and board awareness of the risks associated with outsourcing agreements in order to ensure effective risk management practices;
- Ensuring that an outsourcing arrangement is prudent from a risk perspective and consistent with the business objectives of the institution;
- Systematically assessing needs while establishing risk-based requirements;
- Implementing effective controls to address identified risks;
- Performing ongoing monitoring to identify and evaluate changes in risk from the initial assessment; and
- Documenting procedures, roles/responsibilities, and reporting mechanisms.

Typically, this process incorporates the following activities:

- Risk assessment and requirements definition;
- Due diligence in selecting a service provider;
- Contract negotiation and implementation; and
- Ongoing monitoring.

The preceding comments focus on risk elements specifically associated with outsourcing. For a broader perspective on IT transactional and operational risk, refer to the IT Handbook's "Supervision of Technology Service Providers (TSP) Booklet," which addresses outsourcing risk from the service provider perspective.

Risk Assessment and Requirements

Action Summary

Management should:

- Assess the risk from outsourcing;
- Involve stakeholders in creating risk-based written requirements to control an outsourcing action; and
- Use the written requirements to guide and manage the remainder of the outsourcing process.

Outsourced IT services can contribute to operational risks (also referred to as transaction risks). Operational risk may arise from fraud, error, or the inability to deliver products or services, maintain a competitive position, or manage information. It exists in each process involved in the delivery of the financial institutions' products or services. Operational risk not only includes operations and transaction processing, but also areas such as customer service, systems development and support, internal control processes, and capacity and contingency planning. Operational risk also may affect other risks such as interest rate, compliance, liquidity, price, strategic, or reputation risk as described below.

- Reputation risk-Errors, delays, or omissions in information technology that become public knowledge or directly affect customers can significantly affect the reputation of the serviced financial institutions. For example, a TSP's failure to maintain adequate business resumption plans and facilities for key processes may impair the ability of serviced financial institutions to provide critical services to their customers.
- Strategic risk-Inadequate management experience and expertise can lead to a lack of understanding and control of key risks. Additionally, inaccurate information from TSPs can cause the management of serviced financial institutions to make poor strategic decisions.
- Compliance (legal) risk-Outsourced activities that fail to comply with legal or regulatory requirements can subject the institution to legal sanctions. For example, inaccurate or untimely consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose the institution to civil money penalties or litigation. TSPs often agree to comply with banking regulations, but their failure to track regulatory changes could increase compliance risk for their serviced financial institutions.
- Interest rate, liquidity, and price (market) risk-Processing errors related to investment income or repayment assumptions could lead to unwise investment or liquidity decisions thereby increasing market risks.

Quantity of Risk Considerations

The quantity of risk associated with an outsourced IT service is subject to the function outsourced, the service provider, and the technology used by the service provider. Management should consider the following factors in evaluating the quantity of risk at the inception of an outsourcing decision.

- Risks pertaining to the function outsourced include:
  - Sensitivity of data accessed, protected, or controlled by the service provider;
  - Volume of transactions; and
  - Criticality to the financial institution's business.
- Risks pertaining to the service provider include:
  - Strength of financial condition;
  - Turnover of management and employees;
  - Ability to maintain business continuity;
  - Ability to provide accurate, relevant, and timely Management Information Systems (MIS);
  - Experience with the function outsourced;
  - Reliance on subcontractors;
  - Location, particularly if cross-border (See Appendix C, Foreign-Based Third-Party Service Providers); and
  - Redundancy and reliability of communication lines.
- Risks pertaining to the technology used include:
  - Reliability;
  - Security; and
  - Scalability to accommodate growth.

Requirements Definition

The definition of business requirements sets the stage for all outsourcing actions and forms the basis for subsequent management of the outsourced activity. The requirements are developed through a process that identifies the functions or activities to be outsourced, assesses the risk of outsourcing those functions or activities, and establishes a baseline from which appropriate control measures can be identified. These requirements provide a basis for an understanding between the financial institution and the service provider as to what the risks are and how they will be managed and controlled.

Key Practices

Sound practices for the development of requirements include:

- Stakeholder involvement-All organizational groups who will be directly involved with the service provider or in using the contracted service should be represented in the development of product and service requirements.
- Integration-The development should result in requirements that support the subsequent steps of solicitation, selection, contracting, and monitoring.
- Documentation-Documentation will greatly assist in ensuring that the service contracted and delivered meets the institution's requirements. Documentation will also allow for subsequent reviews of the processes' adequacy and integrity.

Components

The requirements definition phase should result in a detailed document containing descriptions of the institution's expectations relative to the outsourced service. The requirements document may consider, but is not limited by, the following high level topical components:

- Scope and nature
  - Service description;
  - Technology; and
  - Customer support.
- Standards and service levels
  - Availability and performance;
  - Change management;
  - Financial reporting;
  - Quality of service;
  - Security; and
  - Business continuity.
- Minimum acceptable service provider characteristics
  - Industry experience;
  - Management experience;
  - Technology and systems architecture;

    - Process controls;
    - Financial condition;
    - Reputation, including references;
    - Degree of reliance on third parties, subcontractors, or partners;
    - Legal, regulatory, and compliance history; and
    - Ability to meet future needs.
- Monitoring and reporting
    - Measurements and reporting criteria;
    - Right to audit;
    - Third-party reports; and
    - Coordination of responses to security events.
- Transition requirements
    - Initial migration of data to the service provider;
    - Implementation of necessary communications mechanisms;
    - Migration of data from the service provider at termination of contract; and
    - Staff training.
- Contract duration, termination, and assignment
    - Start and term;
    - Conditions and right to cancel;
    - Ownership of data;
    - Timely return of data in machine-readable format;
    - Costs of transition;
    - Limitations, as appropriate, governing assignment to third party;
    - Dispute resolution; and
    - Confidentiality of institution data.
- Contractual protections against liability
    - Indemnification;
    - Limitation of liability; and
    - Insurance.

When outsourcing to a subsidiary or affiliate is considered, management must assure that the components outlined above evidence an arms-length transaction. An arrangement between a financial institution and an affiliate or subsidiary should be on terms that are substantially the same, or at least as favorable to the institution, as those prevailing at the time for comparable transactions with a non-affiliated third party.

Service Provider Selection

Action Summary

Management should:

- Evaluate service provider proposals in light of the institution's needs, including any differences between the institution's solicitation and the service provider proposal;
- Perform due diligence on the prospective service providers;
- Ensure that selection of affiliated parties as service providers is done at arms length in accordance with regulations and guidance issued by the institution's primary regulator; and
- Evaluate foreign-based third-party service providers in light of the guidance found in this section and in Appendix C, Foreign-Based Third-Party Service Providers.

After identifying the work to be performed and the necessary controls, a financial institution solicits responses from prospective service providers. The primary tool for the solicitation is the Request for Proposal (RFP). The RFP also supports subsequent contract negotiations.

Request for Proposal

A financial institution should generate the RFP from the information developed during the requirements definition phase. While the level of detail may vary for any particular procurement, the RFP should describe the institution's objectives; the scope and nature of the work to be performed; the expected production service levels, delivery timelines, measurement requirements, and control measures; and the financial institution's policies

for security, business continuity, and change control. It also requests responses addressing those requirements as well as the fees each service provider will charge.

Once management distributes the RFPs and receives responses, it should evaluate the service provider proposals against the institution's needs. When the institution evaluates the proposals, it may find that the proposals do not completely agree with the RFP. For example, the service the service provider proposes may include different processing workflows or reporting schemes, pricing formulas or techniques, or the response to information requests may not be complete. If the institution considers proposals that differ from the RFP, the institution should evaluate the differences against its requirements and clearly understand how the changes will affect the institution's objectives and service expectations. The institution should evaluate material differences using a process similar to the one used to develop the requirements initially. An institution should negotiate a resolution to any differences between the RFP and the service provider proposal before contracting with a service provider.

Due Diligence

A financial institution should perform due diligence on the service provider's response to an RFP as well as the service provider itself. Due diligence should serve as a verification and analysis tool, providing assurance that the service provider meets the institution's needs. Due diligence should confirm and assess the following information regarding the service provider:

- Existence and corporate history;
- Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate;
- Other companies using similar services from the provider that may be contacted for reference;
- Financial status, including reviews of audited financial statements;
- Strategy and reputation;
- Service delivery capability, status, and effectiveness;
- Technology and systems architecture;
- Internal controls environment, security history, and audit coverage;
- Legal and regulatory compliance including any complaints, litigation, or regulatory actions;
- Reliance on and success in dealing with third party service providers;
- Insurance coverage; and
- Ability to meet disaster recovery and business continuity requirements.

Other important elements include probing for information on intangibles, such as the third party's service philosophies, quality initiatives, and management style. The culture, values, and business styles should fit those of the financial institution. When a foreign-based service provider is considered, the evaluation should assess the relationship in light of the above items as well as the information discussed in Appendix C, Foreign-Based Third-Party Service Providers.

Financial institutions may perform due diligence on one or more of the service providers that respond to the RFP. The depth and formality of the due diligence performed may vary according to the risk of the outsourced relationship, the institution's familiarity with the prospective service providers, and the stage of the provider selection process.

Once institutions issue RFPs, receive and evaluate responses, and perform due diligence, they enter into contract negotiations with one or more of the service providers they have determined can best meet their needs.

Contract Issues

Action Summary

Before signing a contract, management should:

- Ensure the contract clearly defines the rights and responsibilities of both parties;
- Ensure the contract contains adequate and measurable service level agreements;
- Ensure contracts with affiliates clearly reflect an arms-length relationship and costs and services are at least as favorable to the institution as those available from a non-affiliated provider;
- Choose the most appropriate pricing method for the financial institution's needs;
- Ensure the contract does not contain provisions or inducements that may have a significant, adverse affect on the institution;
- Engage legal counsel to review the contract; and
- Evaluate foreign-based third-party service providers in light of the guidance found in this section and in Appendix C, Foreign-Based Third-Party Service Providers.

After selecting a service provider, management should negotiate a contract that meets their requirements. The RFP and the service provider's response can be used as inputs to this process. The contract is the legally binding document that defines all aspects of the servicing relationship. A written contract should be present in all servicing relationships. This includes instances where the service provider is affiliated with the

institution. When contracting with an affiliate, the institution should ensure the costs and quality of services provided are commensurate with those of a nonaffiliated provider. The contract is the single most important control in the outsourcing process. Because of the importance of the contract, management should:

- Verify the accuracy of the description of the outsourcing relationship in the contract;
- Ensure the contract is clearly written and contains sufficient detail to define the rights and responsibilities of each party comprehensively; and
- Engage legal counsel early in the process to help prepare and review the proposed contract.

Examples of contract elements that should be considered include:

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

- Descriptions of required activities, timeframes for their implementation, and assignment of responsibilities. Implementation provisions should take into consideration other existing systems or interrelated systems to be developed by different service providers (e.g., an Internet banking system being integrated with existing core applications or systems customization);
- Obligations of, and services to be performed by, the service provider including 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; and
- Guidelines for adding new or different services and for contract re-negotiation.

Performance Standards. Institutions should include performance standards that define 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. Also see the Service Level Agreements section in this booklet.

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). [4] 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, and 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 verify that the service provider complies with all applicable requirements 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 intrusions occur, the effect on the institution, and corrective action to respond to the intrusion, based on agreements between both parties.

Controls. Management should consider implementing contract provisions that address the following controls:

- Service provider internal controls;
- Compliance with applicable regulatory requirements;
- Record maintenance requirements for the service provider;
- Access to the records by the institution;
- Notification requirements and approval rights for any material changes to services, systems, controls, key project personnel, and service locations;
- Setting and monitoring parameters for financial functions including payments processing or extensions of credit on behalf of the institution; and
- Insurance coverage maintained by the service provider.

Audit. The institution should include in the contract the types of audit reports it is entitled to receive (e.g., financial, internal control, and security reviews). The contract should specify the audit frequency, any charges for obtaining the audits, as well as the rights of the institution and its regulatory agencies to obtain the results of the audits in a timely manner. The contract may also specify rights to obtain documentation of the resolution of any deficiencies and to inspect the processing facilities and operating practices of the service provider. Management should consider, based upon the risk assessment phase, if it can rely on internal audits or if there is a need for external audits and reviews.

For services involving access to open networks, such as Internet-related services, management should pay special attention to security. The institution should consider including contract terms requiring periodic control reviews performed by an independent party with sufficient expertise. These reviews may include penetration testing, intrusion detection, reviews of firewall configuration, and other independent control reviews. The institution should receive sufficiently detailed reports on the findings of these ongoing audits to assess security adequately without compromising the service provider's security.

Reports. Contractual terms should include the frequency and type of reports the institution will receive (e.g., performance reports, control audits, financial statements, security, and business resumption testing reports). The contracts should also outline the guidelines and fees for obtaining custom reports.

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. The contracts should outline the service provider's responsibility to test the plans regularly and provide the 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 a copy of the contingency plan that outlines the required operating procedures in the event of business disruption. 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. Institutions should be aware of and approve all subcontractors. To provide accountability, the financial institution should designate the primary contracting service provider in the contract. The contract should also specify that the primary contracting service provider is responsible for the services outlined in the contract regardless of which entity actually conducts the operations. The institution should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.

Cost. The contract should fully describe the calculation of fees for base services, including any development, conversion, and recurring services, as well as any charges based upon volume of activity or for special requests. Contracts should also address the responsibility and additional cost for purchasing and maintaining hardware and software. Any conditions under which the cost structure may be changed should be addressed in detail including limits on any cost increases. Also see the Pricing Methods and Bundling sections in this booklet.

Ownership and License. The contract should address the ownership, rights to, and allowable use of the institution's data, equipment/hardware, system documentation, system and application software, and other intellectual property rights. Ownership of the institution's data must rest clearly with the institution. 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. Additional information regarding the development of customized software to support outsourced services can be found in the IT Handbook's "Development and Acquisition Booklet."

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 a provision for a dispute resolution process that attempts to resolve problems in an expeditious manner as well as a provision for continuation of services during the dispute resolution period.

Indemnification. Indemnification provisions should require the service provider to hold the financial institution harmless from liability for the negligence of the service provider. Legal counsel should review these provisions to ensure the institution will not be held 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, management should assess 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. Management should assess the timeliness and expense of contract termination provisions. The extent and flexibility of termination rights can vary depending upon the service. Institutions should consider including termination rights 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. The contract should establish notification and timeframe requirements and provide for the timely return of the institution's data and resources in a machine readable format upon termination. Any costs associated with conversion assistance should also 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. Assignment provisions should also reflect notification requirements for any changes to material subcontractors.

Foreign-based service providers. Institutions entering into contracts with foreign-based service providers should consider a number of additional contract issues and provisions. See Appendix C included in this booklet.

Regulatory Compliance. Financial institutions should ensure that contracts with service providers include an agreement that the service provider and its services will comply with applicable regulatory guidance and requirements. The provision should also indicate that the service provider agrees to provide accurate information and timely access to the appropriate regulatory agencies based on the type and level of service it provides to the financial institution.

Service Level Agreements (SLAs)

Service level agreements are formal documents that outline the institution's pre-determined requirements for the service and establish incentives to meet, or penalties for failure to meet, the requirements. Financial institutions should link SLAs to provisions in the contract regarding incentives, penalties, and contract cancellation in order to protect themselves against service provider performance failures.

Management should develop SLAs by first identifying the significant elements of the

service. The elements can be related to tasks (i.e., processing error rates, system up-time, etc.) or they can be organizational (i.e., employee turnover). Once it has identified the elements, management should devise ways to measure the performance of those elements objectively. Finally, institutions should determine the frequency of the measurements and an acceptable range of results to determine when a service provider violates the SLA benchmarks.

Although the specific performance standards may vary with the nature of the service delivered, management should consider SLAs to address the following issues:

- Availability and timeliness of services;
- Confidentiality and integrity of data;
- Change control;
- Security standards compliance, including vulnerability and penetration management;
- Business continuity compliance; and
- Help desk support.

SLAs addressing business continuity should measure the service provider's or vendor's contractual responsibility for backup, record retention, data protection, and the maintenance of disaster recovery and contingency plans. The SLAs can also test the contingency plan's provisions for business recovery timeframes or conducting periodic tests of the plan. Neither contracts nor SLAs should contain any extraordinary provisions that would excuse the vendor or service provider from implementing its contingency plans (outsourcing contracts should include clauses that discuss unforeseen events for which the institution would not be able to adequately prepare).

Pricing Methods

Financial institutions should have several choices when it comes to pricing an outsourcing venture. Management should consider all available pricing options and choose the most appropriate for the specific contract. Examples of different pricing methods include:

- Cost plus-The service provider receives payment for its actual costs, plus a predetermined profit margin or markup (usually percentage of actual costs). For example, the service provider builds a website at a cost of $5,000 plus a 10% markup; the institution pays $5,500.
- Fixed price-The service provider price is the same for each billing cycle for the entire contract period. The advantage of this approach is that institutions know exactly what the provider will bill each month. Problems may arise if the institution does not adequately define the scope or the process. Often, with the fixed price method, the service provider labels services beyond the defined scope as additional or premium

services. For example, if a service provider bills an institution $500 per month for maintaining a website, and the institution decides it wants to add another link, the service provider may charge more for that service if it is not clearly defined in the original contract.

- Unit pricing-The service provider sets a rate for a particular level of service, and the institution pays based on usage. For example, if an institution pays $.10 per hit on a website, and the site has 5,000 hits for the month, the institution pays $500 for the month.
- Variable pricing-The service provider establishes the price of the service based on a variable such as system availability. For example, the provider bills the institution $500, $600, or $800 per month for service levels of 99.00, 99.50, or 99.75 percent system availability, respectively. If a website was available 99.80 percent of the time in a billing period, the institution would pay $800.
- Incentive-based pricing-Incentives encourage the service provider to perform at peak level by offering a bonus if the provider performs well. This plan can also require the provider to pay a penalty for not performing at an acceptable level. For example, the institution wants a service provider to build a website. The service provider agrees to do so within 90 days for $5,000. The institution offers the provider $6,500 if the website is ready within 45 days, but states that it will only pay $3,500 if the provider fails to meet its 90 day deadline.
- Future price changes-Service providers typically include a provision that will increase costs in the future either by a specified percentage or per unit. Some institutions may also identify circumstances under which price reductions might be warranted (i.e., reduction in equipment costs).

Bundling

The provider may entice the institution to purchase more than one system, process, or service for a single price - referred to as "bundling." This practice may result in the institution getting a single consolidated bill that may not provide information relating to pricing for each specific system, process, or service. Although the bundled services may appear to be cheaper, the institution cannot analyze the costs of the individual services. Bundles may include processes and services that the institution does not want or need. It also may not allow the institution to discontinue a specific system, process, or service without having to renegotiate the contract for all remaining services.

Contract Inducement Concerns

Financial institutions should not sign servicing contracts that contain provisions or inducements that may adversely affect the institution. Such contract provisions may include extended terms (up to 10 years), significant increases in costs after the first few years, and/or substantial cancellation penalties. In addition, some service contracts improperly offer inducements that allow an institution to retain or increase capital by deferring losses on the disposition of assets or avoiding expense recognition. These inducements may attract institutions wanting to mask capital problems.

Inducements can take several forms including the following examples:

- The service provider purchases certain assets (e.g., computer equipment or foreclosed real estate) at book value (which exceeds market value) or purchases capital stock from the institution.
- The service provider offers cash bonuses to the institution upon completion of the conversion.
- The service provider offers up-front cash to the institution. The provider states that the institution acquires the right to future cost savings or profit enhancements that will accrue to the institution because of greater operational efficiencies. These improvements are usually without measurable benchmarks.
- The institution defers expenses for conversion costs or processing fees under the terms of the contract.
- Low installation and conversion costs in exchange for higher future systems support and maintenance costs.

These inducements may offer a short-term benefit to the institution. However, the provider usually recoups the costs by charging a premium for the processing services. These excessive fees may adversely affect an institution's financial condition over the long-term. Furthermore, institutions should account for such inducements in accordance with generally accepted accounting principles (GAAP) and regulatory reporting requirements.

Accordingly, when negotiating contracts, an institution should ensure the provider furnishes a level of service that meets the needs of the institution over the life of the contract. The institution must ensure it accounts for contracts in accordance with GAAP. Contracting for excessive servicing fees and/or failing to account properly for such transactions is an unsafe and unsound practice. In entering into service agreements, institutions must ensure accounting under such agreements reflects the substance of the transaction and not merely the form.

Ongoing Monitoring

Action Summary

Management should monitor service provider performance and potential changes in institution requirements throughout the life of the contract. Monitoring should encompass:

- Key service level agreements (SLAs) and contract provisions;
- Financial condition of the service provider;
- General control environment of the service provider through the receipt and

review of audit reports and other internal control reviews; and

- Potential changes due to the external environment.

Financial institutions should have an oversight program to ensure service providers deliver the quantity and quality of services required by the contract. The monitoring program should target the key aspects of the contracting relationship with effective monitoring techniques. The program should monitor the service provider environment including its security controls, financial strength, and the impact of any external events. The resources to support this program will vary depending on the criticality and complexity of the system, process, or service being outsourced.

To increase monitoring effectiveness, management should periodically rank service provider relationships according to risk to determine which service providers require closer monitoring. Management should base the rankings on the residual risk of the relationship after analyzing the quantity of risk relative to the controls over those risks. Relationships with higher risk ratings should receive more frequent and stringent monitoring for due diligence, performance (financial and/or operational), and independent control validation reviews. Personnel responsible for provider oversight should have the necessary expertise to assess the risks and should maintain suitable documentation. Management should use the oversight documentation when renegotiating contracts as well as developing contingency planning requirements.

User groups are another mechanism financial institutions can use to monitor and influence their service provider. User groups can participate and influence service provider testing (i.e., security, disaster recovery, and systems) as well as promote client issues. Independent user groups can monitor and influence a service provider better than its individual clients. Collectively, the group will constitute a significant portion of the service provider's business.

Key Service Level Agreements and Contract Provisions

Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability. These SLAs formalize the performance criteria against which the quantity and quality of service should be measured. Management should closely monitor the service provider's compliance with key service level agreements. To ensure an effective oversight program, the institution should develop:

- A formal policy that defines the SLA program;
- An SLA monitoring process;

- A recourse process for non-performance;
- An escalation process;
- A dispute resolution process; and
- A termination process.

Financial Condition of Service Providers

Institutions should have on-going monitoring of the financial condition of their provider(s). To fulfill its fiduciary responsibility, an institution involved in an outsourcing arrangement should determine the financial viability of its provider(s) on an annual basis. However, if the financial condition of the provider is declining or unstable, more frequent financial reviews are warranted. Once the financial review is complete, management should report the results to the board of directors or to a designated committee. At a minimum, management's review should contain a careful analysis of the provider's annual financial statement. Institution management may also use other forms of information to determine a provider's condition, such as independent auditor reports. These reports may contain information that can be vital in determining a provider's financial condition. Managers also can use information provided by public media (trade magazines, newspapers, television, etc.).

If the institution becomes aware that the provider's financial condition is unstable or deteriorating, the institution should implement its contingency plan. Even if the provider remains in operation, its financial problems may jeopardize the quality of its service and possibly the integrity of the data in its possession. Institutions should consider a provider's failure to provide adequate financial data as a potential red flag that there may be serious financial stability issues.

Termination of services due to the bankruptcy of the service provider can have a devastating effect on a serviced institution's operations. There may not be sufficient advance notice of termination, an effective contingency plan, or adequate access to provider personnel. In such a situation, the serviced institution is put into the position of having to find an alternate processing site with little advance notice.

At this point, a serviced institution has several alternatives including:

- Paying off the servicer's creditor(s) and hiring outside specialists to operate the center;
- Obtaining required equipment and software for in-house processing; and
- Transferring data files to another provider.

Most options are costly and may cause harmful operating delays.

In some instances, the provider owns the programs and documentation required to process the institution's files. Unless the contract contains an escrow agreement for

source code, the program and documentation are unavailable to the institution. These programs are often the TSPs only significant assets. Therefore, a creditor of a bankrupt TSP, in an attempt to recover outstanding debts, might seek to attach those assets and further limit their availability to institutions. The bankruptcy court may provide remedies to the institution, but only after adjudicating substantive matters.

General Control Environment of the Service Provider

To oversee the risks associated with the use of external providers effectively, the institution should evaluate the adequacy of a provider's internal and security controls. Management should ensure the provider develops and adheres to appropriate policies, procedures, and standards. When conducting its evaluation, the institution should consider the results of internal audits conducted by institution staff or a user group, as well as external audits and control reviews conducted by qualified sources The IT Handbook's "Audit Booklet" provides additional details on the various types of external audit engagements for third-party audits of a service provider.

The institution's review of the audit should include an assessment of the following factors in order to determine the adequacy of a service provider's internal and security controls:

- The practicality of the service provider having an internal auditor, and the auditor's level of training and experience;
- The service providers external auditors' training and background; and
- Internal IT audit techniques of the service provider.

Financial institutions should conduct a regular, comprehensive audit of their service provider relationships. The audit scope should include a review of controls and operating procedures that help protect the institution from losses due to irregularities and willful manipulations.

Third-party review reports generated on external providers typically identify certain internal control measures that client institutions are responsible for implementing in order for the provider's accounting systems to be effective. These client institution internal control measures are essential. Financial institution management and audit personnel should verify that the recommended institution internal controls are working effectively, and that the controls effectively complement the accounting system controls described in the provider's third-party review.

Because of the need for an effective internal control program, designated personnel should periodically perform "around-the-computer" audit techniques that:

- Develop data controls (proof totals, batch totals, document counts, number of accounts, and pre-numbered documents) at the institution before submission to the provider. The auditor should sample the controls periodically to ensure their accuracy.

- Include spot-checking reconcilement procedures to ensure output totals agree with input totals, less any rejects.
- Sample rejected, un-posted, holdover, and suspense items to determine why they did not process and how they are addressed (to assure they are properly corrected and reentered on a timely basis).
- Verify selected master file information (such as service charge codes), review exception reports, and crosscheck loan extensions and deposit account entries to source documents.
- Spot-check computer calculations, such as loan rebates, interest on deposits, late charges, service charges, and past-due loans.
- Trace transactions to final disposition to ensure there are adequate audit trails.
- Review source input to ensure sensitive master-file change requests have the required prior approval by appropriate staff or management.
- Visit the provider periodically to assess the status of controls.
- Review other provider audits.

In addition, "through-the-computer" audit techniques allow the auditor to use the computer to check processing steps. These techniques use audit software programs to test extensions and footings and to prepare direct verification statements. These audit software programs often can invoke statistical sampling routines in generating their audit confirmations. If a serviced institution has audit software, it should make arrangements with the provider to allow its use.

Regardless of whether the information processing is internal or outsourced, the financial institution's board of directors should ensure adequate audit coverage. If the institution has no technical audit expertise, the non-technical audit methods can provide minimum coverage. The institution should supplement the internal audit with comprehensive outside IT audits.

Potential Changes due to the External Environment

The contract between the institution and the service provider should be written to encompass the institution's requirements at the time the contract is formed. Over time, the institution's needs may change due to changes in regulation, the economic environment, competition, and other factors outside the contract. Although the contract should provide for flexibility to meet those changing needs, the institution should monitor for changes and update its contract accordingly.

Related Topics

Business Continuity Planning

Action Summary

Financial institutions should:

- Establish ongoing and effective business continuity and information security monitoring programs;
- Effectively manage multiple service provider relationships; and
- Assess, monitor, and effectively control cross-border risks when foreign service providers are used.

Each financial institution should have an effective business continuity plan as outlined in the IT Handbook's "Business Continuity Planning Booklet." The financial institution should also establish ongoing effective business continuity monitoring programs to ensure TSPs adequately control the risks, including information security aspects, associated with the technology services provided. The financial institution has responsibility not only for those portions of the business continuity program performed in-house, but for any portions of the plan developed by a service provider or otherwise outsourced. Financial institutions should consider TSP-related business continuity programs when developing internal plans and programs.

The outsourcing risk management program should identify, for Business Continuity Planning (BCP) purposes, the specific responsibilities of all parties, particularly in the areas of information security and business continuity planning. Financial institutions must also consider which of their critical financial services rely on TSP services, including key telecommunication and network service providers.

The institution should understand all relevant service provider business continuity requirements, incorporate those requirements within its own business continuity plan, and ensure the service provider tests its plan annually. Management should require the service provider to report all test plan results and to notify the institution after any business continuity plan modifications. The institution should integrate the provider's business continuity plan into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan.

Many financial institutions rely on outside data processing providers and any extended interruption or termination of service can disrupt normal operations. Termination of services should occur according to the terms of the service contract, but can result from unanticipated events.

If the provider complies with basic industry standards and maintains an effective business continuity plan, disruption of services should be minimal and the contract will remain intact. The business continuity plan should require the provider to maintain current data files and programs at an alternative site and arrange for processing at another location. At a minimum, these provisions should allow the provider to process the most important data applications. The institution's business continuity plan, which should complement the provider's plan, is an essential recovery tool when disruption occurs with minimal advance notice.

Events that can cause interruption in the availability of an institution's technology include natural disasters, accidents, software errors, hardware failure, utility outages, and social, political, and economic instability. Even with an outsourcing arrangement, the institution should ensure appropriate backup provisions have been established for their critical data and related processing functions. Effective backup procedures will allow the institution to continue processing applications in the event the data communication system fails. Numerous options are available for management to consider, such as using batch rather than real-time processing methods, operating PCs in an offline mode, capturing data at the controller if transmission lines are lost, or altering communication links through redundant data communication lines, backup modems, or rerouted circuits from the local telephone carrier. Institutions that perform data capture or other functions in-house, should address alternative sites or other means in their backup plan to recover or continue these functions.

Regardless of the method used, an institution should have a comprehensive backup plan with procedures that detail how to obtain and use personnel and equipment. Institutions should test backup capabilities periodically to ensure protection is available and employees are familiar with the plan.

With respect to monitoring and maintaining business continuity plans, institutions should:

- Regularly review the business continuity plans of the service provider or vendor to ensure any services considered "mission critical" for the financial institution could be restored within an acceptable timeframe.
- Review the service provider's program for contingency plan testing. For critical services, annual or more frequent tests of the contingency plan are required.
- Assess service provider/vendor interdependencies for mission critical services and applications.

Outsourcing the Business Continuity Function

In addition to ensuring that outsourced financial and technology services include appropriate business continuity plans; financial institutions that outsource all or a portion of their business continuity capability should consider the following factors.

- Staffing-The provider should have sufficient and knowledgeable staff available to provide appropriate onsite technical support to ensure timely resumption of operations at the recovery site.
- Processing Time Availability-The provider should allocate sufficient processing time, resources, and security controls to accommodate the potential for multiple clients. The institution should ensure it could process normal volumes of work within appropriate time requirements.
- Access Rights-The provider should disclose any access limitations. The provider should guarantee the institution's right to use the site in case of an emergency.

Alternatively, the institution should understand any priority arrangements. For example, some sites operate on a first-come, first-serve basis until the site is at full capacity, but others have pre-arranged priorities based on contractual agreements.

- Hardware and Software-The recovery site should have compatible hardware and software. The institution should monitor the compatibility of the site to handle its specific computer hardware and software requirements. To facilitate the monitoring, the provider should be required by contract to notify the institution of any changes in the hardware, software, and equipment at the recovery site.

- Security Controls-The institution should ensure it can maintain adequate physical and logical security controls at the recovery site.

- Testing-The service provider contract should address access to the recovery site for periodic testing. At a minimum, the institution needs sufficient access to perform at least one full-scale test of the recovery site annually, including verification of telecommunications capabilities. Similarly, the institution should ensure the service provider also performs periodic tests of its own BCP and submits test results to customer financial institutions.

- Confidentiality of Data-The institution should ensure the provider can maintain the confidentiality of its business and customer data. The service provider should maintain controls sufficient to ensure the security and confidentiality of the information assets consistent with the institution's information security program. Confidentiality of data is particularly important when multiple clients operate from the same recovery site. Institution management should establish whether the service provider has addressed these issues in its contract, particularly the provisions concerning the Interagency Guidelines Establishing Standards for Safeguarding Customer Information. [5]

- Telecommunications-The institution should review telecommunications redundancy and capacity at the recovery site, including how communications from the institutions to the recovery site will be established. The service provider should take steps to ensure the recovery site will have adequate telecommunications services (both voice and data) for all of its clients.

- Reciprocal Agreements-Financial institutions contracting with another institution for a recovery site should consider the above issues of staffing, processing availability, access rights for recovery or testing, compatibility, security, capacity, etc. Both institutions should ensure they maintain sufficient capacity to meet recovery time objectives and minimum service levels in the event one institution needs to recover operations

- Space-The recovery site should have adequate space to accommodate the affected institution's recovery staff.

- Printing Capacity / Capability-The recovery site should maintain adequate printing capacity to meet the demand of the affected institution under acceptable levels of service.

- Contacts-Institution management should know the procedures for declaring a disaster including who has the authority to declare a disaster and initiate use of the recovery site. Also, the institution should maintain an updated list of contacts names and numbers for the recovery site provider and know the procedures for communicating with the provider.

Outsourced business continuity arrangements can be cost-effective for smaller institutions when compared to establishing and maintaining dedicated alternate recovery sites. Institutions should periodically conduct a thorough test of outsourced disaster recovery services (at least annually).

Information Security/Safeguarding

Information assets are valuable, and institutions should ensure these assets are adequately protected in outsourcing relationships. Financial institutions have a legal responsibility to ensure service providers take appropriate measures designed to meet the objectives of the information security guidelines, and comply with GLBA 501 (b). Those measures should result from the institution's security process and should be included or referenced in the contract between the institution and the service provider. Refer to the IT Handbook's "Information Security Booklet" for additional information on the information security process.

In choosing service providers, management should exercise appropriate due diligence to ensure the protection of both financial institution and customer assets. Before entering into outsourcing contracts, and throughout the life of the relationship, institutions should ensure the service provider's physical and data security standards meet or exceed standards required by the institution. Institutions should also implement adequate protections to ensure service providers and vendors are only given access to the information and systems that they need to perform their function. Management should restrict their access to financial institution systems, and appropriate access controls and monitoring should be in place between service provider's systems and the institution.

Multiple Service Provider Relationships

A multiple service provider relationship is an environment where two or more service providers collaborate to deliver an end-to-end solution to the financial institution.

An institution can select from two techniques to manage this relationship, but remains responsible for understanding and monitoring the control environment of all servicers that have access to the financial institution's systems, records, or resources. The first technique involves the use of a lead service provider to manage the institution'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 or stand-alone contracts. If the first technique is employed, management should ensure its primary service provider has a contractual obligation to notify the financial institution of any concerns (controls / performance) associated with any of its outsourced activities. Management should also ensure the service provider's control environment meets or exceeds the institution's expectations, including the control environment of organizations that the primary service provider utilizes.

Stand-alone contracts with each service provider require increased management of each provider. Contracting for a technology solution by using one lead provider may lessen the need for the institution to become directly involved if subcontractors fail to perform, but it does not diminish the responsibility for monitoring the internal and security controls of subcontractors through the primary service provider relationship. Because the institution has less control using the lead provider approach, management should require by contract that TSPs notify the institution of all subcontractor relationships.

Outsourcing to Foreign Service Providers

Some institutions develop outsourcing relationships with service providers located in foreign countries. These arrangements can provide cost, expertise, and other advantages to the institutions and should be subject to the same due diligence and assessment as domestic outsourcing relationships. In addition, foreign outsourcing relationships result in unique strategic, reputation, credit, liquidity, transactional, geographic, and compliance risks that institutions should identify, assess, prevent, and control. See Appendix C for additional detail.

Endnotes

[1] See 12 USC 1867 (c)(1) and 12 USC 1464 (d)(7). The NCUA does not currently have independent regulatory authority over TSPs.

[2] S. Rep. No. 2105, 87-2105 at 3 (1962). reprinted in 1962 U.S.C.C.A.N. 3878, 3880. Accord H.R. Rep. No. 105-417, at 4 (1998), reprinted in 1998 U.S.C.C.A.N. 22. 23.

[3] Institutions may find advantages in contracting for services for three or more years because of the costs of en-tering into the contract, the costs of changing service providers, and favorable price breaks that may be offered by the vendor for longer terms. Contract flexibility is necessary under these circumstances because of the rapid changes occurring in an IT environment. Contract flexibility should allow for changes in service levels; increase or decrease in the scope of the process, service, or system due to changing institutional goals or objectives; and the retargeting of all relational elements on an annual basis. See Contract Inducement Concerns section in this booklet for further issues to be considered in entering into long-term contracts.

[4] The "Guidelines Establishing Standards to Safeguard Customer Information" to implement section 501(b) of the Gramm-Leach- Bliley Act of 1999 (GLBA) promulgated by the FFIEC agencies requires institutions to, among other things, require service providers by contract to implement appropriate security controls to comply with the guidelines with respect to their handling of customer information.

[5] See 66 Federal Register 8616 (Feb. 1, 2001); 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F. (Board); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS). See 66 Federal Register 8152 (Jan. 30, 2001); 12 CFR Part 748, app. A (NCUA).

[6] The terms "foreign-based third-party service providers" or "foreign-based service provider" refer to any entity, including an affiliated organization or holding company, whose servicing operations are located in and subject to the laws of any country other than the United States, including service providers located outside the United States providing services to foreign branches of U.S. organizations. The term also includes the foreign opera-tions, whether by subcontract or otherwise, of a domestic service provider.

[7] 15 USC 6801. Gramm-Leach-Bliley Act, Section 501(b).

[8] In this regard, organizations using foreign-based service providers should be aware of Section 319 of the USA Patriot Act, Pub. L. No. 107-56 (Oct. 26, 2001), which requires a financial institution to make information on anti-money laundering compliance by the institution or its customers available within 120 hours of a government request.

[9]	Organizations should identify and understand the application of any laws within a foreign jurisdiction that apply to information transferred from the United States to that foreign jurisdiction over the Internet or otherwise to information transferred from that jurisdiction to the United States, as well as to information collected within the foreign jurisdiction using automated or other equipment in that jurisdiction.
[10]	The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against certain foreign countries, organizations sponsoring terrorism, and international narcotics traffickers based on U.S. foreign policy and national security goals. For more information, refer to the OFAC Web site at www.treas.gov/ofac.
[11]	Export controls on commercial encryption products are administered by the Bureau of Industry and Security, part of the Department of Commerce. Organizations may be exporters if they provide encryption software to a foreign-based service provider, but some exceptions are available that apply to foreign national employees, in-cluding contractors and consultants, of U.S. companies and their subsidiaries inside and outside the United States. Export administration regulations regarding encryption are contained in 15 CFR §§ 740.13, 740.17 & 742.15. See www.bis.doc.gov.
[12]	12 CFR part 364, Appendix B, III.D.2 - Banks and 12 CFR part 570, Appendix B, III (d)(2)- Thrifts.
[13]	12 CFR part 332 - Banks and 12 CFR part 573 - Thrifts.
[14]	The term "U.S. regulatory authorities" means the FFIEC member agencies issuing this booklet.
[15]	12 USC 1867(c)(1) - Banks and 12 USC 1464(d)(7)- Thrifts. In addition, organizations should notify their primary regulatory authority of a service relationship with a foreign-based service provider in accordance with regulations and guidance issued by that regulator.
[16]	In instances where the financial institution's foreign branches have outsourced local operations or services cross-border to third-party service providers domiciled in another foreign country, copies of such records can be maintained at the foreign branch office, but must also be available in the U.S.

Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Assess the effectiveness of the institution's risk management process as it relates to the outsourcing of information systems and technology services.

- Tier I objectives and procedures relate to the institution's implementation of a process for identifying and managing outsourcing risks.
- Tier II objectives and procedures provide additional validation and testing techniques as warranted by risk to verify the effectiveness of the institution's process on individual contracts.

Tier I and Tier II are intended to be a tool set examiners will use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the appropriate scope for the examination.

1. Review past reports for weaknesses involving outsourcing. Consider:

- Regulatory reports of examination of the institution and service provider(s); and
- Internal and external audit reports of the institution and service provider(s) (if available).

2. Assess management's response to issues raised since the last examination. Consider:

- Resolution of root causes rather than just specific issues; and
- Existence of any outstanding issues.

3. Interview management and review institution information to identify:

- Current outsourcing relationships, including cloud computing relationships, and changes to those relationships since the last examination. Also identify any:

  - Material service provider subcontractors,

- Affiliated service providers,
- Foreign-based third party providers;

- Current transaction volume in each function outsourced;
- Any material problems experienced with the service provided;
- Service providers with significant financial or control related weaknesses; and
- When applicable, whether the primary regulator has been notified of the outsourcing relationship as required by the Bank Service Company Act or Home Owners' Loan Act.

Objective 2: Evaluate the quantity of risk present from the institution's outsourcing arrangements.

1. Assess the level of risk present in outsourcing arrangements. Consider risks pertaining to:

- Functions outsourced;
- Service providers, including, where appropriate, unique risks inherent in foreign-based service provider arrangements; and
- Technology used.

2. If the institution engages in cloud computing, determine whether:

- The cloud computing service is or will be hosted internally or outsourced to a third party provider (hosted externally).
- Resources are shared within a single organization or across various clients of the service provider. (Resources can be shared at the network, host, or application level).
- The institution has the ability to increase or decrease resources on demand without involving the service provider (on-demand self-service).
- Massive scalability in terms of bandwidth or storage is available to the institution.
- The institution can rapidly deploy or release resources.
- The financial institution pays only for those resources which are actually used (pay-as-you go pricing)

3. If the institution engages in cloud computing, identify the type(s) of service model that is or will be used:

- Software as a Service (SaaS) - application software is hosted in the cloud; commonly used for email applications such as Hotmail or Gmail, time reporting systems, customer relationship management (CRM) systems such as SalesForce, etc.;
- Platform as a Service (PaaS) - development platform such as Java, .Net, etc. for developing systems is hosted in the cloud;
- Infrastructure as a Service (IaaS) - infrastructure resources such as data processing, data storage, network systems, etc. are provided via the cloud; or
- Data as a Service (DaaS) - data is provided or accessed via the cloud such as access to LexisNexis data, Google data, and Amazon data

4. If the institution engages in cloud computing, identify the type of deployment model to be used:

- Private Cloud - hosted for or by a single entity on a private network; can be hosted internally or outsourced but is most often operated internally; only those within the entity share the resources;
- Community Cloud - hosted for a limited number of entities with a common purpose; access is generally restricted; most often used in a regulated environment where entities have common requirements;
- Hybrid Cloud - data or applications are portable and permit private and public clouds to connect; or,
- Public Cloud - available to the general public; owned and operated by a third party service provider

Objective 3: Evaluate the quality of risk management 1. Evaluate the outsourcing process for appropriateness given the size and complexity of the institution. The following elements are particularly important:

- Institution's evaluation of service providers consistent with scope and criticality of outsourced services; and
- Requirements for ongoing monitoring.

2. Evaluate the requirements definition process.

- Ascertain that all stakeholders are involved; the requirements are developed to allow for subsequent use in request for proposals (RFPs), contracts, and monitoring; and actions are required to be documented; and
- Ascertain that the requirements definition is sufficiently complete to support the future control efforts of service provider selection, contract preparation, and monitoring.

3. Evaluate the service provider selection process.

- Determine that the RFP adequately encapsulates the institution's requirements and that elements included in the requirements definition are complete and sufficiently detailed to support subsequent RFP development, contract formulation, and monitoring;
- Determine that any differences between the RFP and the submission of the selected service provider are appropriately evaluated, and that the institution takes appropriate actions to mitigate risks arising from requirements not being met; and
- Determine whether due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, reputation (e.g., reference checks), controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities and use of subcontractors.

4. Evaluate the process for entering into a contract with a service provider. Consider whether:

- The contract contains adequate and measurable service level agreements;
- Allowed pricing methods do not adversely affect the institution's safety and soundness, including the reasonableness of future price changes;
- The rights and responsibilities of both parties are sufficiently detailed;
- Required contract clauses address significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, subcontractors, continuity of service, etc;

- Legal counsel reviewed the contract and legal issues were satisfactorily resolved; and
- Contract inducement concerns are adequately addressed.

5. If the institution engages in cloud processing, determine that inherent risks have been comprehensively evaluated, control mechanisms have been clearly identified, and that residual risks are at acceptable levels. Ensure that

- Action plans are developed and implemented in instances where residual risk requires further mitigation.
- Management updates the risk assessment as necessary.
- The types of data in the cloud have been identified (social security numbers, account numbers, IP addresses, etc.) and have established appropriate data classifications based on the financial institution's policies.
- The controls are commensurate with the sensitivity and criticality of the data.
- The effectiveness of the controls are tested and verified.
- Adequate controls exist over the hypervisor if a virtual machine environment supports the cloud services.
- All network traffic is encrypted in the cloud provider's internal network and during transition from the cloud to the institution's network.
- All data stored on the service providers systems are being encrypted with unique keys that only authenticated users from this institution can access.
- Unless the institution is using private cloud model, determine what controls the institution or service provider established to mitigate the risks of multitenancy.
- If a financial institution is using the Software as a Service (SaaS) model, determine whether regular backup copies of the data are being made in a format that can be read by the financial institution. (Backup copies made by the service provider may not be readable.)
- Ensure that the financial institution's business continuity plan addresses contingencies for the cloud computing service. Determine whether the financial institution has an exit strategy and de-conversion plan or strategy for the cloud services.
- Determine whether the cloud service provider has an internal IT audit staff with adequate knowledge and experience or an adequate contractual arrangement with a qualified third-party audit firm.

6. Evaluate the institution's process for monitoring the risk presented by the service provider relationship. Ascertain that monitoring addresses:

- Key service level agreements and contract provisions;
- Financial condition of the service provider;
- General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports;
- Service provider's disaster recovery program and testing;
- Information security;
- Insurance coverage;
- Subcontractor relationships including any changes or control concerns;
- Foreign third party relationships; and
- Potential changes due to the external environment (i.e., competition and industry trends).

7. Determine whether the following policies and processes have been revised in light of the need for increased controls brought about by the implementation of cloud computing:

- The Information Security Risk Assessment;
- The Technology Outsourcing (Vendor Management) Policy;8. Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment). Decision process should:
- The Information Security Policy;
- The Security Incident or Customer Notification Policy;
- The Business Continuity Plan

8. Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment). Decision process should:

- Include objective criteria;
- Support consistent application;
- Consider the degree of service provider support for the institution's strategic and critical business needs, and
- Specify subsequent actions when rankings change.

9. Evaluate the financial institution's use of user groups and other mechanisms to monitor and influence the service provider.

Objective 4: Discuss corrective action and communicate findings

1. Determine the need to complete Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. Review preliminary conclusions with the EIC regarding:

- Violations of law, rulings, regulations;
- Significant issues warranting inclusion in the Report as matters requiring attention or recommendations; and
- Potential impact of your conclusions on the institution's risk profile and composite or component IT ratings.

3. Discuss findings with management and obtain proposed corrective action for significant deficiencies.

4. Document conclusions in a memo to the EIC that provides report ready comments for the Report of Examination and guidance to future examiners.

5. Organize work papers to ensure clear support for significant findings by examination objective.

TIER II OBJECTIVES AND PROCEDURES

A. IT REQUIREMENTS DEFINITION

1. Review documentation supporting the requirements definition process to ascertain that it appropriately addresses:

- Scope and nature;

- Standards for controls;
- Minimum acceptable service provider characteristics;
- Monitoring and reporting;
- Transition requirements;
- Contract duration, termination, and assignment' and
- Contractual protections against liability.

B. DUE DILIGENCE

1. Assess the extent to which the institution reviews the financial stability of the service provider:

- Analyzes the service provider's audited financial statements and annual reports;
- Assesses the provider's length of operation and market share;
- Considers the size of the institution's contract in relation to the size of the company;
- Reviews the service provider's level of technological expenditures to ensure on-going support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

2. Evaluate whether the institution's due diligence considers the following:

- References from current users or user groups about a particular vendor's reputation and performance;
- The service provider's experience and ability in the industry;
- The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;
- The quality and effectiveness of any cost/benefit analyses. Determine whether the analysis considered the incremental costs of the additional monitoring, operations responsibilities, and protections that may be required of the financial institution.
- The cost for additional system and data conversions or interfaces presented by the various vendors;
- Shortcomings in the service provider's expertise that the institution would need to

supplement in order to fully mitigate risks;

- The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities;
- The service provider's ability to respond to service disruptions;
- Key service provider personnel that would be assigned to support the institution;
- The service provider's ability to comply with appropriate federal and state laws. In particular, ensure management has assessed the providers' ability to comply with federal laws (including GLBA and the USA PATRIOT Act); and
- Country, state, or locale risk.

C. SERVICE CONTRACT

1. Verify that legal counsel reviewed the contract prior to closing.

- Ensure that the legal counsel is qualified to review the contract particularly if it is based on the laws of a foreign country or other state; and
- Ensure that the legal review includes an assessment of the enforceability of local contract provisions and laws in foreign or out-of-state jurisdictions.

2. Verify that the contract appropriately addresses:

- Scope of services;
- Performance standards;
- Pricing;
- Controls;
- Financial and control reporting;
- Right to audit;
- Ownership of data and programs;
- Confidentiality and security;
- Regulatory compliance;
- Indemnification;
- Limitation of liability;
- Dispute resolution;

- Contract duration;
- Restrictions on, or prior approval for, subcontractors;
- Termination and assignment, including timely return of data in a machine-readable format;
- Insurance coverage;
- Prevailing jurisdiction (where applicable);
- Choice of Law (foreign outsourcing arrangements);
- Regulatory access to data and information necessary for supervision; and
- Business Continuity Planning.

3. Review service level agreements to ensure they are adequate and measurable. Consider whether:

- Significant elements of the service are identified and based on the institution's requirements;
- Objective measurements for each significant element are defined;
- Reporting of measurements is required;
- Measurements specify what constitutes inadequate performance; and
- Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

4. Review the institution's process for verifying billing accuracy and monitoring any contract savings through bundling.

D. MONITORING SERVICE PROVIDER RELATIONSHIP(S)

1. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:

- Timeliness of review, given the risk from the relationship;
- Changes in the risk due to the function outsourced;
- Changing circumstances at the service provider, including financial and control

environment changes;

- Conformance with the contract, including the service level agreement; and
- Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.

2. Review risk rankings of service providers to ascertain:

- Objectivity;
- Consistency; and
- Compliance with policy.

3. Review actions taken by management when rankings change, to ensure policy conformance when rankings reflect increased risk.

4. Review any material subcontractor relationships identified by the service provider or in the outsourcing contracts. Ensure:

- Management has reviewed the control environment of all relevant subcontractors for compliance with the institution's requirements definitions and security guidelines; and
- The institution monitors and documents relevant service provider subcontracting relationships including any changes in the relationships or control concerns.

Platform as a Service (PaaS) - development platform such as Java, .Net, etc. for developing systems is hosted in the cloud;

- Infrastructure as a Service (IaaS) - infrastructure resources such as data processing, data storage, network systems, etc. are provided via the cloud; or,
- Data as a Service (DaaS) - data is provided or accessed via the cloud such as access to LexisNexis data, Google data, and Amazon data.

Appendix B: Laws, Regulations, and Guidance

Laws

- 12 USC 1464 (d) (7): Home Owners' Loan Act (Thrifts) (N/A)
- 12 USC 1867 (c) (11): Bank Service Company Act (Banks) (N/A)
- 15 USC 6801: Gramm-Leach-Bliley Act (N/A)
- Pub. L. No. 107-56: USA PATRIOT Act (N/A)

Federal Reserve Board

- SR 00-4 (SUP): Outsourcing of Information and Transaction Processing (February 2000)
- SR 00-17 (SPE): Guidance on the Risk Management of Outsourced Technology Services (November 30, 2000)

Federal Deposit Insurance Corporation

- FIL-49-99: Bank Service Company Act (June 3, 1999)
- FIL-50-2001: Bank Technology Bulletin: Technology Outsourcing Information Documents (June 4, 2001)

National Credit Union Administration

- NCUA Letter to Credit Unions No. 02-CU-17: E-Commerce Guide for Credit Unions (December 2002)
- NCUA Letter to Credit Unions No. 01-CU-20: Due Diligence Over Third Party Service Providers (November 2001)

Office of the Comptroller of the Currency

- OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers (May 15, 2002)
- OCC Bulletin 2001-47: Third-Party Relationships, Risk Management Principles (November 1, 2001)

Office of Thrift Supervision

- 12 CFR Part 570, Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
- CEO Letter 113: Internal Controls (July 14, 1999)
- Thrift Activities Handbook: Section 340: Internal Control (December 2003)
- Thrift Activities Handbook: Section 341: Technology Risk Controls (October 1997)

Appendix C: Foreign-Based Third-Party Service Providers

The material provided in this appendix focuses on foreign-based third-party service providers and should be used, in addition to all other material in this booklet, when examining such relationships. This appendix discusses the primary risks that may arise from service relationships between financial institutions and foreign-based third-parties [6] ,the steps institutions should consider when managing those risks, and the implications of the relationships within the context of the examination process.

BACKGROUND

Organizations often use domestic third-party service providers as an economic alternative to internal technology and data processing functions. Increasingly, these organizations are considering arrangements with foreign-based third parties or domestic firms that subcontract portions of their operations to foreign-based entities.

The use of foreign-based service providers is a common business practice that can be a less costly alternative to self-processing or to using domestic service providers. However, this practice raises country, compliance, contractual, reputation, operational (e.g., transactional), and strategic issues in addition to those presented by use of a domestic service provider. In managing these issues, management should conduct appropriate risk assessments and due diligence procedures and closely evaluate all contracts. Additionally, management should establish ongoing monitoring and oversight procedures.

RISK MANAGEMENT

A financial institution's senior managers are responsible for understanding the risks associated with foreign-based relationships and for ensuring that effective risk management practices are in place. Management should determine if a foreign-based technology relationship is consistent with the organization's overall business and technology strategies and if it can mitigate identified risks adequately. Before management executes a contract with foreign-based entities, it should consider issues such as choice-of-law and jurisdictional considerations. Additionally, organizations should establish appropriate due diligence and risk management policies that include oversight and monitoring procedures. These policies and procedures should consider that all of the risks associated with domestic third party providers are present in foreign-based arrangements in addition to the unique issues such as country and compliance risks arising from the fact that the third parties may not fall under the jurisdiction of domestic laws and regulations.

COUNTRY RISK

Country risk is an exposure to economic, social, and political conditions in a foreign country that could adversely affect a vendor's ability to meet its service level requirements. In certain situations, country risks could result in the loss of an organization's data, research, or development efforts. Managing country risk requires organizations to gather and assess information regarding foreign political, social, and economic conditions and events, and to address the exposures introduced by the relationship with a foreign-based provider. Risk management procedures should include the establishment of contingency, service continuity, and exit strategies in the event of unexpected disruptions in service.

COMPLIANCE RISK

Compliance risk involves the impact foreign-based arrangements could have on an organization's compliance with applicable U.S. and foreign laws and regulations. An organization's use of a foreign-based third party service provider should not inhibit the organization's compliance with applicable U.S. laws including consumer protection, privacy (Section 501(b) of GLBA) [7] , and information security laws as well as Bank Secrecy Act requirements [8] concerning the reporting and documentation of financial transactions. Additionally, organizations should consider the impact and operational requirements of foreign data privacy laws or regulatory requirements [9] .Organizations engaging foreign-based entities should also consider the sanctions and embargo provisions [10] of the U.S. Treasury Office of Foreign Assets Control (OFAC) as well as the requirements regarding exportation of encryption-related technologies discussed in the following paragraph.

Export Controls

The United States has export control laws that restrict the export of software and other items (U.S. Export Administration Regulations). [11] These laws apply to all aspects of encryption usage, including but not limited to, software, hardware, and network applications. Organizations should ensure they and their service provider(s) comply with these laws. Contracts should include a representation and warranty that service providers will comply with U.S. export control laws.

DUE DILIGENCE

Management of an organization considering a foreign-based outsourcing arrangement should perform appropriate due diligence similar to domestic outsourcing arrangements before selecting or contracting with a service provider. The process should include an evaluation of a firm's financial stability and commitment to service, and the potential impact of the foreign jurisdiction's regulations, laws, accounting standards, and business practices. Additionally, management should consider the degree to which geographic distance, language, or social, economic, or political changes may affect the foreign-based service provider's ability to meet the organization's servicing needs. Management should consider the cost and logistical implications of managing a cross-border relationship, including the ongoing costs of managing and monitoring cross-border and foreign-based provider relationships.

CONTRACTS

Contracts between an organization and a foreign-based entity should address the risks identified during risk assessments and due diligence processes. Specific topics that should be considered regarding such contracts are discussed in the following paragraphs.

Security, Confidentiality and Ownership of Data

Management should require contract provisions to protect its customers' privacy and the confidentiality of organizational records in conformance with U.S. laws and regulations. Federal regulations require that service provider contracts include provisions requiring the service provider to implement procedures and security measures that meet the objectives of customer information security guidelines. [12] Additionally, contracts should include provisions prohibiting the disclosure of any customer information to nonaffiliated third parties, other than as permitted under U.S. privacy laws. [13]

Any agreement with a foreign-based service provider should also include a provision that all information transferred to the foreign-based entity remains the property of the organization, regardless of how it is processed, stored, copied, or reproduced.

Regulatory Authority

Arrangements with foreign-based service providers should contain a provision acknowledging the authority of U.S. regulatory authorities [14] (pursuant to the Bank Service Company Act or the Home Owner's Loan Act) to examine the services performed by the provider. [15] Financial institutions must not share U.S. regulatory examination reports or information contained therein with either foreign regulators or foreign-based service providers without the express written approval of the appropriate U.S. regulatory authority.

Choice Of Law

Before entering into an agreement or contract with a foreign-based vendor or developer, an organization should carefully consider which country's law it wishes to control the relationship. Based on that review, organizations should include choice of law and jurisdictional covenants that provide for the resolution of disputes between the parties under the laws of a specific jurisdiction.

These provisions are necessary to maintain continuity of service, access to data, and protection of customer information. For these reasons, it can be particularly important when dealing with foreign service providers to specify exactly which country's laws will control the contractual relationship between the parties. Additionally, contract provisions may be subject to foreign-court interpretations of local laws. The laws of the foreign country may not recognize choice of law provisions and may differ from U.S. law regarding what they require of organizations or how they protect bank customers. Thus, an organization's due diligence should include analysis of a country's local laws by legal counsel competent in assessing the enforceability of all aspects of a contract.

MONITORING AND OVERSIGHT

Monitoring foreign entities requires the same steps as monitoring domestic servicers and vendors in addition to the recommendations presented within this appendix. When organizations establish a servicing arrangement with a foreign-based service provider, management should monitor both the entity and the conditions within the foreign country.

The organization should determine that the foreign-based service provider maintains adequate physical and data security controls, transaction procedures, business resumption and IT contingency arrangements (including periodic testing), insurance coverage, and compliance with applicable laws and regulations. Further, where indicated by the organization's security risk assessment, the organization must monitor its foreign-based service providers to confirm that they have satisfied security obligations imposed in the contract to comply with Section 501(b) of GLBA.

Organizations also should monitor economic and governmental conditions within the foreign country to determine whether changes are likely to affect the ability of the service provider to perform under the arrangement.

REGULATORY AGENCY ACCESS TO INFORMATION

U.S. regulatory authorities must have the ability to examine the services performed by an organization's third-party service provider regardless of whether it is foreign or domestically based. Organizations must maintain, in the files of a U.S. office, appropriate English language documentation to support all arrangements with service providers. Appropriate documentation typically includes a copy of the contract establishing the arrangement, supporting legal opinions, due diligence reports, audits, financial statements, performance reports, and other critical information. [16] In addition, the organization should have an appropriate contingency plan to ensure continued access to critical information, to maintain service continuity, and the resumption of business functions in the event of unexpected disruptions or restrictions in service resulting from transaction, financial, or country risk developments.

EXAMINATION CONSIDERATIONS

U.S. regulatory authorities may examine the services performed for an organization under an outsourcing arrangement with a foreign-based service provider. Likewise, in the case of a foreign-regulated entity, U.S. regulatory authorities may be able to obtain information through the appropriate supervisory agency in the service provider's home country.

With respect to the outsourcing organization in such arrangements, U.S. regulatory authorities will focus reviews on the adequacy of an organization's due diligence efforts, its risk assessments, and the steps taken to manage those risks including the effect of the arrangement upon the organization's compliance with applicable laws and its access to critical information. Regulatory reviews will assess the organization's contract provisions and its ongoing monitoring or oversight program, including any internal and

external audits arranged by the foreign-based service provider or the organization.

An organization's use of a foreign-based third-party service provider (and the location of critical data and processes outside of U.S. territory) must not compromise the ability of U.S. regulatory authorities to effectively examine the organization. Thus, organizations should not establish servicing arrangements with entities where local laws or regulations would interfere with U.S. regulatory agencies' full and complete access to data or other relevant information. Any analysis of foreign laws obtained from counsel should include a discussion regarding regulatory access to information for supervisory purposes.

Appendix D: Managed Security Service Providers

Background and Purpose

A growing number of financial institutions (FIs) are partially or completely outsourcing the security management function to third parties, typically known as Managed Security Service Providers (MSSPs). FIs engage MSSPs due to increasingly sophisticated threats, cost pressures, and absence of internal expertise. The services that MSSPs provide present additional risks FIs are required to manage.

The purpose of this appendix is to identify the risks associated with the MSSP engagement and offer guidance to assist FIs in mitigating these risks. While the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) on Information Security Booklet provides related guidance, FIs should pay particular attention to risk management issues that are heightened when serviced by MSSPs. The loss of control that comes with the outsourced security function introduces an element of risk that FIs need to understand and appropriately manage. The following subsection, MSSP Engagement Criteria covers numerous engagement criteria and related contract considerations institutions should consider when engaging an MSSP.

In addition to the normal vendor management responsibilities, a successful engagement with an MSSP should include:

- A contract with mutually agreed upon Service Level Agreements (SLAs);

  Strategies for ensuring transparency and accountability that include:

o Regular communication between the FI and the MSSP on

matters inncluding change control, problem resolution,

threat assessments, and MIS reporting,

o Descriptions of processes for physical and logical controls over

FI data; and,

- Periodic review of the MSSP's processes, infrastructure, and control environment through offsite reviews of documentation and onsite visitations.

Types of Managed Security Services

Following are some of the many types of security-related services offered by MSSPs:

- Network Boundary Protection

  Using technology such as firewalls and virtual private networks (VPNs), the MSSP protects the FI's network perimeter. The MSSP should provide device monitoring of connections to external third parties such as Internet Service Providers.

- Management of Intrusion Detection and Prevention for Networks and Hosts

  Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are automated services that can detect patterns in network traffic and may take action according to a rule set or pattern definition database.

- Event Log Management and Alerting

  Event log management and alerting is conducted to monitor event logs generated by network devices or computer systems to centralize, filter, and provide management reports on material activity. Alerts can be set for highly sensitive events or activities.

- Anti-virus and Web Content Filtering Services

  Managed antivirus protection provides organizations with malware protection that helps safeguard FIs from new threats. The malware definitions are updated frequently to help recognize the new threats.

- Patch Management and Security Software Management

  MSSPs can identify and manage network security related software systems and

components requiring regular security updates; conduct compatibility testing before deployment; deploy the updates uniformly; and provide reporting on the status and effectiveness of the security software as implemented.

- Security Incident Response and Management

  MSSPs can assist an organization in building an incident response team or providing a turnkey incident response in the event of a breach.

- Data Leak Prevention

  MSSPs can help identify all methods of data ingress and egress, and establish systems that monitor and enforce appropriate controls.

- Secure Messaging

  MSSPs can provide services to ensure the security of messages into and out of the FI.

- Information Security Consulting Services

  Security consulting by MSSPs may include risk assessment, vulnerability assessment testing, penetration testing, compliance tools, education and training, and attestation services.

Description of Managed Security Services Arrangements

Managed security services arrangements can include the following four deployment models:

- Full Outsourcing: Under this model the MSSP performs the following functions autonomously.

o Manage all network connections at customer premises;

o Manage network platforms;

o Update rules and thresholds over networking devices;

o Analyze data and necessary escalation responses; and

o Provide client reports or alerts on outcomes of the managed

service.

- Co-managed: Under this model the FI and MSSP use the same infrastructure and have access rights and responsibilities on platforms.

o Typically involves client-owned network equipment on their

premises;

o Includes common security event monitoring tools and data loss

prevention solutions; and

o IDS/IPS events are reported to the MSSP and the FI consults

with the MSSP providing primary services during off hours.

- Split Processing: Under this model, the MSSP performs some functions and the FI performs others.

o Most commonly used with firewall and network devices where the

MSSP monitors log data, health and capacity with the FI pushing

system updates, rules changes, or configurations;

o Vulnerability assessment and analysis where the MSSP and FI

each test applications and platforms; and

o Sometimes used when multiple MSSPs are employed.

- Consulting: Consulting services provided by MSSPs can include assisting with risk assessments, initial system configuration, policy formulation, compliance (PCI, GLBA, and SOX), forensics, penetration testing, application security testing, application code review, social engineering, physical security, and management reporting.

Governance

Effective governance is fundamental for understanding and managing the risks involved when outsourcing to MSSPs. Critical areas include availability, integrity, and confidentiality of FI data. The costs to procure, operate, and manage service delivery, including review for compliance with the SLAs, should be part of the overall contract.

Risk Assessment

A risk assessment must be performed as part of, or in conjunction with, the due diligence review when an FI is considering outsourcing security services. Concerns about vendors become especially important as security practices that were traditionally conducted in-house are outsourced to an MSSP. The MSSP risk assessment should guide the FI as it develops, implements, tests, and maintains the information systems security program.

Financial Institution Requirements

Gathering necessary information internally and from the potential MSSP is necessary to identify potential threats, vulnerabilities, and controls. Documentation of the risk assessment is especially important to help ensure coordination, consistency, and standardization between the FI and the MSSP. The identification of information systems and the ranking of sensitive data and applications at the MSSP should be part of the risk assessment process. Coordination is also necessary to help ensure that vulnerabilities are identified and processes are validated through testing.

Risk Considerations for Managed Security Services

The reliance on MSSPs may significantly increase an FI's risk profile. Increased risk can arise from poor planning, lack of oversight and control, and/or poor MSSP performance or service. To control these risks, the FI should exercise appropriate due diligence prior to entering an MSSP relationship and maintain effective governance during the relationship.1

Below are risk elements that should be considered in an FI's MSSP risk assessment.2 The risks identified are relevant regardless of the type of MSSP arrangement.

Risk Elements Pertaining to Managed Security Services

- Business Process

  According to the FI's risk profile, the following risks should be considered:

o Decline in business reputation and customer confidence;

o Liability under business partnership agreements;

o False sense of security by FI management;

o Diverse offshore legal, geo-political, and cultural risk;

o Impact on competitive advantage when valuable intellectual property or proprietary information is stolen;

o Reputational damage should the MSSP fail to provide the contracted service;

o Heightened legal and regulatory issues;

o Dependence on an outside organization for critical services;

o Loss of the FI experience, knowledge, and skill development; and

o Vendor financial condition decline.

Information Security Infrastructure

To optimize service availability while mitigating risks, the following should be considered:

o Complexity of network infrastructure and deployment of agents;

o Information security breaches and data loss;

o Loss to the FI for failing to comply with applicable regulations

and laws;

o Downtime due to lack of resilient MSSP infrastructure; and

o Loss of the FI's key control requirements due to MSSP's "one

size fits all" products.

- Access Management and Control

  Ensure FI and MSSP user access is monitored, controlled, and assessed for inappropriate or inadequate:

o MSSP access of FI data;

o User access controls;

o Segregation of duties;

o Control and oversight of MSSP activity by the FI; and

o Attestations of MSSP access to FI systems and data.

- Protection Against Malware

  To protect the computing environment of malicious software the MSSP should have the following:

o Current antivirus/malware protection;

o Strong patch and/or configuration management policies

and procedures;

o Timely identification of compromised devices; and

o Appropriate endpoint protection tools.

- Data and Media Handling

  To foster adequate data and media handling protection, consider if the MSSP has:

o Proper application configuration;

o Secure data storage and/or processing by MSSPs;

o Adequate access and integrity controls;

o Appropriate encryption;

o Adequate key management for encrypted data; and

o Sufficient data retention.

- Application Development and Systems Integration

  An FI should confirm that application development and change management are performed securely by an MSSP. The following should be considered:

o Configuration specifications;

o Change management processes at the MSSP and/or at the FI;

o Logging and monitoring; and

o Recertification of software and permissions.

- Business Continuity and Disaster Recovery

  An FI should confirm that MSSPs can provide resilient services in the event of an outage or disruption. Risks that FIs should identify and address include:

o Incompatible continuity plans and unrealistic disaster recovery

planning;

o Insufficient distance between datacenter and backup datacenter

(or recovery cite) for disaster recovery;

o Inadequate disaster recovery testing and postmortem report

(Disaster recovery is not in line with disaster recovery needs.);

o Poor communication between the FI and MSSP during

a disaster; and

o Inadequate capacity of the MSSP to service all clients during an outage.

- Incident Response Management

  An FI should identify, monitor, and manage incidents in coordination with the MSSP. Risks that FIs should identify and address include:

o Undefined roles and responsibilities between the FI and the MSSP;
o Untimely reporting of incidents and/or data breaches;
o Failure to take appropriate steps to contain and control the incident;
o Failure to notify the FI's customers or regulators on FI's behalf per contract agreement;
o Failure to perform joint incident response table-top testing with MSSPs;
o Overdependence on the MSSP for incident response; and
o Legal issues arising from a security incident involving both parties.

- Awareness and Training

  An FI should determine that all parties are aware of and trained in processes and MIS reports. Potential risks to be addressed include:

o Insufficient training or expertise at either the MSSP or FI; and
o Inadequate MSSP personnel screening practices.

Request for Information and Request for Proposal

Request for Information (RFI) and Request for Proposal (RFP) are part of a deliberate and intentional process associated with engaging an MSSP. This type of evaluation should be completed in accordance with the FI's strategic plan and tactical approach to security. For example, the strategic plan should determine what security functions to maintain in-house, whether to contract a sole provider, or split services between providers. The RFI, the initial formal step in selection, must define FI objectives for the service needed. These objectives primarily are to be based on the FI's configuration (OS, security, network, and servers) and security policies. The FI should also consider the MSSP's staffing, certifications, training, transition process, and incident response methodology.

It is essential for the FI to coordinate with the MSSP regarding configuration and staff resources. This will be important not only to initial selection through the RFI/RFP and contracting process, but as the relationship evolves. It is important that the MSSP be a cultural fit with the FI. 3 MSSP specific contract language will require modification to RFIs and RFPs based on the FI and vendor configuration. See subsection, MSSP Engagement Criteria for RFI/RFP examples specific to MSSPs.

Initial Due Diligence

An FI considering an MSSP engagement must perform adequate due diligence to validate that the vendor is capable of managing security services that are aligned with their risk profile. Management should consider performing an onsite visitation to determine if the servicer has the appropriate experience and control environment to meet the FI's needs, how long the MSSP has been in business, the MSSP's staffing, the MSSP's incident response methodology, etc.

When performing an onsite visitation, the FI should determine if the MSSP can ensure the security of their data. Pertinent entity and operating information should be obtained to facilitate the vendor selection process. Discussions with management should focus on the risk elements noted in the risk assessment section with emphasis on determining that the MSSP has the necessary expertise and experience to service the FI and will provide sufficient metrics for the FI to assess compliance with the contract.

The time the MSSP has been operating and if there are any expected changes (e.g., merger, acquisitions, expansion/growth, etc.), that could impact contracted services should be determined. The number of clients the MSSP services and number of FI clients also should be identified. If the MSSP does not have FI clients, it may indicate the vendor is seeking to enter into an unfamiliar business area. Before accepting this risk, the MSSP's familiarity with pertinent regulatory requirements such as GLBA, SOX, and FFIEC guidance must be validated.

When evaluating the MSSP's expertise, the following should be considered:

- Current and unbiased customer testimonials and/or references;

- Use of current monitoring and risk management technologies;

- The MSSPs ability to:

o Generate timely MIS reporting and incident notification;

o Maintain confidentiality, integrity, and availability of FI data; and

- Manage prospective services for the defined contract term.

If the MSSP does not perform all services in-house, FIs should determine which services are to be outsourced, the quality of vendor management exercised by the MSSP, and whether the service provider(s) is/are offshore.

To fulfill its duties, an MSSP may be required to install software and/or hardware in an FI's data center. What data will be collected, reviewed, stored, and secured by the MSSP should be defined with established SLAs based on business requirements. The dialog between the MSSP and the FI should focus on identifying services that preserve security.

The initial due diligence process is a key method to determine if an MSSP can provide the necessary services to an FI. Each of the above recommendations should be considered in deciding if the MSSP is viable and has the ability to fulfill the terms of the engagement.

Contracts

In any MSSP arrangement, the contractual expectations and obligations of each party should be clearly defined, understood, monitored, and enforced. FI managers who have a strong understanding of MSSP risks and mitigating controls should be involved in contract development. Legal representatives with the expertise to assess the enforceability and legitimacy of MSSP contract terms should review contract provisions and be included in contract negotiations. The alignment of contract provisions with FI security policies and procedures creates a strong foundation for the development of

comprehensive MSSP agreements.

Although most contract requirements for MSSPs are similar to those of other outsourcing arrangements, FIs should consider the following provisions when developing a formal contract with an MSSP.

Scope of Service

Contract discussion should include:

- Specific services provided, timelines for implementation, and explicit responsibilities of the MSSP and the FI;
- The right to modify existing services performed under the contract;
- The type and frequency of reports available;
- Activities the MSSP is allowed to conduct when operating within the FI network;
- Handling of confidential data;
- Ownership of data generated by proprietary security or third-party monitoring tools owned by the MSSP; and
- Access rights granted to the MSSP as it relates to FI network systems.

Service Level Agreements

Well defined SLAs provide the framework for establishing the expectations and metrics for the effective delivery of service such as levels of availability, performance, or support. When working with MSSPs, attention should be given to the engagement criteria in Appendix A.

Contract Term and Renewal

The role of the MSSP relationship and how the length of the contract integrates with the FI's overall business strategy and objectives should be defined. Long-term contracts may limit flexibility and consideration should be given to whether to accept automatic contract renewal provisions.

Termination

FIs should consider including termination rights for a variety of conditions including material breach, critical performance failure, and material non-performance. Grounds for termination should be clearly defined and agreed on by the FI and service provider. If the contract is terminated for cause, the MSSP should cover damages. The FI's exit strategy should consider post-termination rights including:

- Transfer of data in the FI's preferred format;
- Transfer of FI data or assets from the MSSP and all subcontractors;
- Assistance from the service provider to migrate services in-house or to another provider;
- Right to purchase non-proprietary tools used by the MSSP to provide the services; and
- Timely response to the FI's post-termination requests.

Managing the Relationship

While the initial due diligence is critical to managing the MSSP relationship, ongoing monitoring and oversight is equally important. Risks of the MSSP relationships are generally similar to risks of other outsourcing arrangements that need to be addressed within the FI's vendor management program, but the MSSP relationship has some attributes that may call for a heightened level of (or more targeted) education and training.

Education and Awareness

Effective MSSP oversight requires an FI to maintain adequate in-house technical expertise. This enables the FI to monitor and maintain acceptable risk exposure and confirm the MSSP is fulfilling contractual obligations. Education and awareness for FI employees is necessary to help ensure:

- The MSSP is effectively managing the relevant information security risk;
- Personnel understand the processes, procedures, and protocols of the MSSP, including the use of subcontractors; and
- FI management understands:

o What data the MSSP is collecting and who has access to the

data;

o Information in audit reports and security testing of the MSSP;

and

o How to measure a successful relationship.

Given the high risk and trust of the relationship, the FI should verify that the MSSP is appropriately managing the contracted security services on its behalf. The following should be addressed in the FIs education and awareness program:

- Training, education, and awareness provided by the MSSP to FI employees;
- Identifying and understanding accountable and responsible parties at the FI and MSSP;
- Maintaining the expertise needed to understand metrics and reporting provided by the MSSP; and
- Training frequency for FI employees.

Contract Performance

FI management should have a monitoring process to attest to the MSSP meeting its contractual obligations. This typically entails reviewing items such as SLAs, Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), security event notification, incident response, and any other metrics relative to performance. These items should be included in MSSP reports, and FIs should perform supplemental monitoring as necessary to evaluate contractual performance.

Ongoing Oversight of MSSP Relationship

The critical services provided by MSSPs require a high level of FI oversight throughout the lifecycle of the contracting relationship. Processes should include maintenance of controls established as part of the initial due diligence, including:

- Reviewing:

o MSSP provided MIS reports,

o MSSP audit reports, including SSAE 16 and other independent

assessment reports, and

o Penetration testing and vulnerability assessment test results;

- Performing periodic onsite visitations of the MSSP;

- Monitoring the MSSP's internal risk assessment process; and

- Discussing any concerns related to the above items with MSSP management.

Contingency & Event Planning

Business Continuity Planning

To avoid a gap in service in the event of an MSSP outage, the FI should:

- Review the MSSP's business continuity plans for the ability to provide continuous services to the FI;
- Confirm that MSSPs have tested their business continuity plans at least annually and have forwarded a summary to the FI; and
- Include critical MSSPs in the FI's tabletop exercise or other business continuity testing.

Incident Response

To assess that the FI is fully prepared to respond to incidents, the FI should:

- Develop and maintain an incident response plan which includes a remediation process clearly defining roles and responsibilities between the MSSP and the FI;
- Establish and review processes and procedures to handle communications to and from the MSSP;
- Establish and define event types and response procedures; and
- Include the MSSP in testing of the incident response plan.

Alternative Providers

To prevent gaps in service associated with MSSP failure, the FI should:

- Maintain awareness of alternate providers;
- Develop policies and procedures to outline FI data ownership;

- Have a clear understanding of service provider roles and responsibilities;

- Assess the MSSP for dependencies with critical services; and

- Consider using multiple vendors to provide various MSSP services.

Demarcation of Responsibility

Along with general monitoring and oversight of the MSSP, FIs should have involvement in the operational and policy activities associated with the MSSP. Examples include:

Policy and Procedures

Outsourcing certain security activities does not diminish the need for adequate security polices at the FI. They should coordinate their information security program with the policies, standards, guidelines, and procedures of the MSSP.

Incident Response

The incident response function needs to be coordinated and clearly defined between the FI and MSSP. Notification and escalation requirements regarding incident response should be clearly documented and aligned between the FI and MSSP. The definition of a reportable event should be clear and unambiguous.

Access Controls

Assess controls/methods and audit trails related to the FI's systems, devices, and data being managed by the MSSP.

Physical Security

Typically the MSSP will place devices within the FI (e.g., firewall, IDS, etc.) which the MSSP may own and/or control. FIs should consider appropriate physical security of such

devices regardless of ownership and/or control.

Change Control

There should be a clear process to communicate changes implemented by either the FI or MSSP. Changes can have a material impact on the security environment, and both parties should undergo an adequate change control review. Advanced notification of any changes should be provided whenever possible.

Data Collection/Logging

The FI should maintain awareness of data the MSSP is collecting, how it is stored, and how it is used. The FI should maintain its data or logs separate from other MSSP clients. The MSSP's data collection and security event classification processes should be defined and understood to help in corroborating the integrity of the FI's data and in establishing a more effective log review process.

Metrics and Reporting

The MSSP should provide regular reporting on agreed on performance metrics to the client FI. It is important that qualified FI personnel review these reports to attest that the security controls of MSSPs are operating as expected. Metrics and reporting should include security:

- Events potentially affecting the FI;
- Statistics specific to the FI;
- Intelligence, and;
- Operational statistics and conditions specific to the FI.

Emerging Risks

Cloud computing is an emerging trend in which some of the IT industry's biggest players are investing significant resources. Cloud computing in general is a migration from owned resources to shared resources in which client users receive information technology services on demand from third-party service providers via the Internet "cloud." In cloud environments, a client or customer will relocate their resources such as data, applications, and services to computing facilities outside the corporate firewall, which the end user then accesses via the Internet.

Cloud-based MSSP services may be implemented as part of Internet access services. Examples of "in-the-cloud" services include carrier-based denial of service protection, virtual firewall services, and carrier-provided URL blocking.

When an MSSP offers services that use a cloud computing architecture, the same risks that are specific to non-cloud-based security services apply. However, there are a few additional risk considerations that should be assessed when moving to a cloud computing environment. Areas for FIs to consider when an MSSP uses cloud computing in their managed security services environment include:

- Protecting data in transit to avoid data leakage;
- Securing data at rest so that one data breach within the cloud does not breach the other customer data within the cloud;
- Maintaining compliance with applicable regulatory requirements;
- Complying with foreign government privacy laws when outsourcing is performed offshore;
- Segregating customer data appropriately to comply with audit and legal requirements; and
- Avoiding sharing of authentication credentials to prevent the impersonation of users.

Conclusion

Financial institutions' challenges in dealing with high profile network security breaches, changing technology, malware, system maintenance costs, complexity, and uncertainty surrounding network security have resulted in an increased use of MSSPs. While FIs can leverage the expertise of the MSSP, managing this relationship can be an additional

challenge, particularly when MSSPs have access to confidential or sensitive information that requires increased protection. In addition, FIs can have high levels of risk exposure in the event that an MSSP cannot comply with service level agreements.

As with all outsourcing arrangements FI management can outsource the daily responsibilities and expertise; however, they cannot outsource accountability.

MSSP Engagement Criteria

MSSP: ENGAGEMENT CRITERIA

SLA - Service level agreement

RFI - Request for information

RFP - Request for proposal

* Contract Provisions for consideration

Criteria	Description	Phase	Information/Expectations
Service Availability	Due to the nature of managed security services, it is critical that the service be operational 24x7 to the fullest extent practicable. While an outage to a core banking system (e.g., teller, loan processing, etc.) may be manageable, a momentary failure of a FI's managed security environment could have disastrous consequences.	SLA* RFI/RFP/SLA SLA* SLA RFP/SLA*	Specify recovery time when a service outage occurs MTTR (Mean Time to Recovery) Identify expectations of percentage of system uptime Notification of any planned outages Defined system performance reports Schedule for applicable credits and compensation
Incident Response and Notification	Timely notification and classification of incidents is critical for most MSSP engagements. The severity of the incident and its potential impact must be identified and communicated to appropriate staff. Plans should be comprehensive and customized to the FI in order to minimize the impact of the breach.	SLA RFP/SLA RFP/SLA RFI/RFP/SLA* RFP/SLA* RFP/SLA	Key staff and backups identified with 24x7 availability Defined severity levels with appropriate escalation requirements Maximum timeframe for communicating new problems and action items Review MSSP incident response plan which should specify how incidents will be handled and by whom. Table top testing is vital to ensure MSSP and FI understand their roles in an actual event Consider MSSP forensic analysis procedures
State/Federal Compliance	Existing state and federal law and regulations	RFP*	Ensure MSSP complies with applicable notification requirements for data security/privacy

Criteria	Description	Phase	Information/Expectations
Staffing	MSSPs provide specialized services performed by IT professionals that must have the expertise necessary to identify and respond to current IT security issues.	RFP/SLA	Identification of staff professional certifications (e.g., CISSP, CISM, etc.)
		RFP/SLA	Procedures for background checks and hiring criteria
		RFI/RFP	Describe process for monitoring Security Operations Center (SOC) personnel
		RFI/RFP	Describe procedures for initial and ongoing staff training.
		RFI/RFP	Provide profile of staffing resources (e.g., experience, number of employees, etc.)
Third-Parties and Subcontractors	FIs must protect customer information, sensitive corporate data, and maintain high availability of services regardless of outsourced relationships. This obligation extends to any third parties utilized to deliver their services.	RFI/RFP*	Identify 3rd parties that may be used and describe roles and oversight.
		RFP*	Notification/approval of significant subcontractors

Handling Sensitive Data	In many engagements, MSSPs may have access to non-public customer data and sensitive information about the FI and its operating environment. Depending on the relationship, the FI may no longer have direct control over the data.	SLA* SLA RFI/RFP/SLA RFP/SLA*	Procedures for restricting use of any sensitive data whether in-transit or at rest Procedures for disclosing the loss or unauthorized access to sensitive data Primary location of data processing and storage (US based) Secure storage, retention, and destruction of data should be clearly defined
Service Scalability	The ability to provide scalable services on a near real-time basis is often one of the key factors considered by FIs in choosing an MSSP.	SLA SLA	Regular reporting of capacity-related statistics such as bandwidth utilization, storage used, and percent of system capacity used. Consideration of anticipated rates of capacity growth, storage needs, and seasonal or promotional spikes

Criteria	Description	Phase	Information/Expectations
Disaster Recovery	In the event the MSSP is subject to a disruptive event, it is critical that services to the FIs remain uninterrupted to the fullest extent practicable.	RFP/SLA* RFP/SLA*	Access to MSSPs' business continuity plan and testing results Standards for Mean Time to Recovery (MTTR)
Customer Support	The breadth of issues that may arise in an MSSP engagement may require 24x7 live customer support.	RFP/SLA	Customer support Guaranteed Response Time (GTR)
Hardware Replacement*	Some MSSP services involve installation of a proprietary hardware device at the FI.	SLA* SLA RFP/SLA	Minimum time for delivery of replacement device Backup device Established procedures for onsite support
Training/Education	FIs may not have the staff expertise to understand the information provided by MSSP specialized management and reporting tools.	RFP/SLA RFP/SLA RFP/SLA	Classroom/onsite training Web-based tutorials Consulting services

Technology	MSSPs utilize specialized technology and information resources that are critical to the service offerings.	RFI/RFP SLA RFP RFI/RFP/SLA	Describe methodology used for collecting, reporting, and analyzing threats, vulnerabilities, or possible attacks. Proprietary technology required Changes required to existing network architecture, configuration or systems SDLC procedures for services delivered
Due Diligence (e.g., onsite visits, audits, financial reviews)	MSSPs have evolved rapidly over the past 10 years from the entrepreneurial "garage business" to formal offerings and facilities. Onsite visits and audit reviews throughout the lifecycle can provide a valuable window to ensure services are offered in a safe and secure manner.	RFI/RFP/SLA RFP/SLA RFP*	What recognized audit reports are available for review (e.g., SAS70, SSAE16, etc.) Provision for pre-engagement and periodic site visits. Access to annual financial statements

MSSP Examination Procedures

EXAMINATION PROCEDURES

NOTE: This appendix includes all of the steps in Appendix A, plus unique ones for MSSP's.

EXAMINATION OBJECTIVE: Assess the effectiveness of the institution's risk management process as it relates to the outsourcing of information systems and

technology and security services, and the heightened risks specific to the outsourcing of security services to a Managed Security Services Provider (MSSP).

Tier I and Tier II Objectives and Examination Procedures are intended to be a tool set examiners will use when selecting examination procedures for their particular examinations. Examiners should use these procedures as necessary to support examination objectives.

Tier I Objectives and Procedures relate to the institution's implementation of a process for identifying and managing risks related to outsourcing functions to an MSSP.

Tier II Objectives and Procedures provide additional validation and testing techniques, as warranted by risk, to verify the effectiveness of the institution's process on individual MSSP contracts.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Determine the appropriate scope for the examination.

1. Review past reports for weaknesses involving outsourcing. Consider:

- Regulatory reports of examination of the institution and service provider(s); and

- Internal and external audit reports of the institution and service provider(s).

2. Assess management's response to issues raised since the last

examination.

Consider:

- Resolution of root causes rather than just specific issues; and

- Existence of any outstanding issues.

3. Interview management and review institution information to identify:

- Current outsourcing relationships and changes to those relationships since the last examination. Also identify:Material service provider subcontractors,

Also identify:

o Material service provider subcontractors,

o Affiliated service providers,

o Foreign-based third party providers;

- Current transaction volume for each function outsourced;

- Material problems experienced with the service provided;

- Service providers with significant financial or control-related weaknesses;

  and

- When applicable, whether the primary regulator has been notified of the outsourcing relationship as required by the Bank Service Company Act or Home Owners' Loan Act.

Objective 2: Evaluate the quantity of risk present from the institution's outsourcing arrangements.

1. Assess the level of risk present in outsourcing arrangements. Consider

risks pertaining to or associated with:

- Functions outsourced;

- Service providers, including where appropriate, unique risks inherent in foreign-based service provider arrangements;

- Technologies used;

- Staff qualifications;

- The MSSP's risk assessment program and whether it includes business process, information security infrastructure, related risk assessments, etc.; and

- The frequency of MSSP risk assessments

Objective 3: Evaluate the quality of risk management.

1. Evaluate the outsourcing process for appropriateness, given the size and complexity of the institution. The following elements are particularly important;

- Institution's evaluation of service providers consistent with scope;
-
- Requirements for ongoing monitoring; and
- Determination of whether the Request for Information (RFI) document outlines the security functions the financial institution (FI) intends to incorporate into the contract with an MSSP.

2. Evaluate the requirements definition process.

- Ascertain that all stakeholders are involved; the requirements are developed to allow for subsequent use in Request For Proposals (RFPs), contracts, and monitoring; and actions are required to be documented; and
- Ascertain that the requirements definition is sufficiently complete to support the future control efforts of service provider selection, contract preparation, and monitoring.

3. Evaluate the service provider selection process to determine if:

- An RFI/RFP was completed;

- The FI included RFI/RFP elements appropriate to level of risk;
- The RFP adequately encapsulates the institution's requirements and that elements included in the requirements definition are complete and sufficiently detailed to support subsequent RFP development, contract formulation, and monitoring;
- Any differences between the RFP and the submission of the selected service provider are appropriately evaluated, and that the institution takes appropriate actions to mitigate risks arising from requirements not being met; and
- Due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, reputation (e.g., reference checks), controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities and use of subcontractors.

4. Evaluate the process for entering into a contract with a service provider.

Consider whether:

- The contract contains adequate and measurable service level agreements;
- Allowed pricing methods adversely affect the institution's safety and soundness, including the reasonableness of future price changes;
- The rights and responsibilities of both parties are sufficiently detailed;
- Required contract clauses address significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, subcontractors, continuity of service, etc.;
- Legal counsel reviewed the contract and legal issues were satisfactorily resolved;
- Contract inducement concerns are adequately addressed; and

- Contracts contain the following relative to MSSP engagements:

o Appropriate MIS reporting commensurate with risk;

o Agreed upon privileged access rights;

o Termination rights and appropriate renewal language;

o Timelines for service implementation and explicit responsibilities of the MSSP and the FI;

o The right to modify existing services performed under the contract;

o A security provision in accordance with the FI's security program; and

o Ownership of data generated by proprietary security or third-party monitoring tools owned by the MSSP;

- Determine if the FI has a process to monitor that the MSSP is fulfilling their obligations outlined within the contract (e.g. Service Level Agreements (SLAs), Knowledge Performance Indicators (KPIs)/Knowledge Risk Indicators (KRIs)).

5. Evaluate the overall governance of the MSSP program.

- Appraise senior management support of the use of MSSPs;

- Review reports related to MSSP compliance with FI information security program;

- Assess changes to the information security program arising from the use of MSSPs; and

- Evaluate MIS reports provided to FI from MSSPs.

6. Evaluate the institution's process for monitoring the risk presented by the service provider relationship. Ascertain that monitoring addresses:

- Key service level agreements and contract provisions;
- Financial condition of the service provider;
- General control environment of the service provider through the receipt and review of appropriate audit and regulatory reports;
- Service provider's disaster recovery program and testing;
- Information security;
- Insurance coverage;
- Subcontractor relationships including any changes or control concerns;
- Foreign third party relationships; and
- Potential changes due to the external environment (i.e., competition and industry trends).

7. Review policies regarding periodic ranking of service providers by risk.

The decision process should:

- Include objective criteria;
- Support consistent application;
- Consider the degree of service provider support for the institution's strategic and critical business needs; and
- Specify subsequent actions when rankings change.

8. Evaluate the financial institution's use of user groups and other

mechanisms to monitor and influence the service provider.

Objective 4: Discuss corrective action and communicate findings.

1. Determine the need to complete Tier II Procedures for additional

validation to support conclusions related to any of the Tier I

Objectives.

2. Review preliminary conclusions with the EIC regarding:

- Violations of law, rulings, regulations;
- Significant issues warranting inclusion in the Report as matters requiring attention or recommendations; and
- Potential impact of your conclusions on the institution's risk profile and composite or component IT ratings.

3. Discuss findings with management, and obtain proposed corrective

action for significant deficiencies.

4. Document conclusions in a memo to the EIC that provides report ready comments for the Report of Examination and guidance to future examiners.

5. Organize work papers to ensure clear support for significant findings by examination objective.

TIER II OBJECTIVES AND PROCEDURES

A. IT REQUIREMENTS DEFINITION

1. Review documentation supporting the requirements definition process to ascertain that it appropriately addresses:

- Scope and nature;
- Standards for controls;
- Minimum acceptable service provider characteristics;
- Monitoring and reporting;
- Transition requirements;

- Contract duration, termination, and assignment; and

- Contractual protections against liability.

B. DUE DILIGENCE

1. Assess the extent to which the institution reviews the financial stability

of the service provider:

- Analyzes the service provider's audited financial statements and annual reports;

- Assesses the provider's length of operation and market share;

- Considers the size of the institution's contract in relation to the size of the company;

- Reviews the service provider's level of technological expenditures to ensure on-going support; and

- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

2. Evaluate whether the institution's due diligence considers the following:

- References from current users or user groups about a particular vendor's reputation and performance;

- The service provider's:

o Experience and ability in the industry;
o Experience and ability in handling situations similar to the Institution's environment and operations;
o Shortcomings in the service provider's expertise that the institution may need to supplement in order to fully mitigate risks;
o Proposed use of third parties, subcontractors, or partners to support the outsourced activities;
o A ability to respond to service disruptions;
o Assigning of Key personnel that would support the institution;
o Ability to comply with appropriate federal and state laws.
In particular, ensure management has assessed the providers' ability to comply with federal laws (including GLBA and the USA PATRIOT Act);

- The cost for additional system and data conversions or interfaces presented by the various vendors; and

- Country, state, or locale risk.

3. Evaluate how the FI determines whether the MSSP meets its risk profile.

Consider whether the FI:

- Performed an onsite visitation of the MSSP;Considered business changes at the MSSP;

- Assessed the extent of MSSP use of subcontractors and if any will be performed by an offshore entity; and
- Evaluated controls over sensitive data where offshore subcontracting is performed.

C. SERVICE CONTRACT

1. Verify that legal counsel reviewed the contract prior to signing. Ensure

that:

- Legal counsel is qualified to review the contract particularly if it is based on the laws of a foreign country or other state; and
- Legal review includes an assessment of the enforceability of local contract provisions and laws in foreign or out-of-state jurisdictions.

2. Verify that the contract appropriately addresses:

- Scope of services;
- Performance standards;
- Pricing;
- Controls;
- Financial and control reporting;

- FIs right to audit;

- Ownership of data and programs;

- Confidentiality and security;

- Regulatory compliance;

- Indemnification;

- Limitation of liability;

- Dispute resolution;

- Contract duration;

- Restrictions on, or prior approval for, subcontractors;

- Termination and assignment, including timely return of data in a machine-readable format;

- Insurance coverage;

- Prevailing jurisdiction (where applicable);

- Choice of law (foreign outsourcing arrangements);

- Regulatory access to data and information necessary for supervision; and

- Business Continuity Planning.

3. Review service level agreements to ensure they are adequate and measurable. Consider whether:

- Significant elements of the service are identified and based on the institution's requirements;

- Objective measurements for each significant element are defined;

- Reporting of measurements is required;

- Measurements specify what constitutes inadequate performance; and

- Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

4. Review the institution's process for verifying billing accuracy and monitoring any contract savings through bundling.

D. MONITORING SERVICE PROVIDER RELATIONSHIP(S)

1. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:

- Timeliness of review, given the risk from the relationship;

- Changes in the risk due to the function outsourced;

- Changing circumstances at the service provider, including financial and control environment changes;

- Conformance with the contract, including the service level agreement; and

- Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.

2. Determine if adequate in house expertise exists to manage an MSSP relationship by evaluating:

- FI management's understanding of the MSSP's process, procedures, and protocols;

- Whether the FI has a thorough understanding of the data the MSSP is collecting and whom has access to the data; and

- The training, education, and awareness provided by the MSSP to the FI.

3. Relative to contingency and event planning between the FI and an

MSSP. Evaluate:

- The most recent business continuity test with the MSSP; review the results, lessons learned and issues to be addressed;

- How the FI monitors the MSSP's BCP plan and testing results;

- The process to develop and maintain incident response processes that include the MSSP;

- How the MSSP roles and responsibilities have been established; and

- Provisions in the FI's contingency plan for continuance of processing activities, either in-house or with another vendor, in the event that the vendor is no longer able to provide the contracted services or the arrangement is otherwise terminated unexpectedly.

4. Relative to ongoing monitoring of an MSSP relationship, the

following should be considered:

- Event notification procedures, response time expected, and actions the MSSP will

take to protect the FI;

- Clearly defined support to be provided during and after "events," (e.g., incident response, forensics, etc.);

- How the MSSP provides continuous monitoring of the FI;

- The quality of the management information reports the MSSP provides to the FI; and

o Determine if reports include status of security,

incidents, business continuity plans, and financial

condition.

- How management at the FI is periodically updated regarding MSSP activities. Assess the scope of reporting including risk assessments, information security, significant incidents, business continuity, and financial condition.

5. Review risk rankings of service providers to ascertain:

- Objectivity;

- Consistency; and

- Compliance with policy.

6. Review actions taken by management when risk rankings change,

to ensure policy conformance when rankings reflect increased risk.

7. Review any material subcontractor relationships identified by

the service provider or in the outsourcing contracts. Ensure:

- Management has reviewed the control environment of all relevant subcontractors for compliance with the institution's requirements definitions and security guidelines; and

- The institution monitors and documents relevant service provider subcontracting relationships including any changes in the relationships or control concerns.

8. Determine if there is adequate coordination between the FI's

security policies and the policies/practices of the MSSP.

Consider whether:

- There is clear understanding of responsibility and accountability during a security event (i.e., incident response);

- The FI has considered access controls surrounding the systems, devices and data that the MSSP can access;

- Effective change control processes and communication exist between the FI and MSSP;

- The quality of the log collection of the MSSP and related Security Information and Event Management tools;

- The quality of the physical security around devices that are owned and/or maintained by the MSSP on the FI's premises;

- The FI's data is maintained in separate client logs at the MSSP; and
- Monitoring for security events/incidents is being conducted by the MSSP on a real-time system (e.g., security console)