Office of Thrift Supervision **September 1, 2004**

Department of the Treasury

Thrift Bulletin

TB 82a

Handbooks: **Thrift Activities** **Section: 310**

Subject: **Oversight by the Board of Directors**

Third Party Arrangements

Summary: OTS recognizes that savings associations and their holding companies may benefit from business relationships with third parties. Thrift Bulletin (TB) 82a replaces TB 82, however, it does not replace previous documents that specifically pertain to information technology (IT) functions (CEO Memo No. 201, July15, 2004, FFIEC Information Technology Handbook, Outsourcing Technology Services), and internal audit outsourcing (TB No. 81, "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing," (March 17, 2003)). This Bulletin instead supplements the requirements and standards in these documents and expands the concept to cover other types of third party arrangements. This document provides guidance on third party arrangements, whether they occur between affiliated or unaffiliated entities.

This update:

- Clarifies the definition of "significant" contracts.
- Clarifies the responsibilities of the board of directors and management.
- Modifies the notification requirement when contracting with foreign service providers.

OTS continues to expect directors and management (you) to effectively manage risks that arise from all types of third party arrangements. OTS examiners will review your internal controls and management of third party arrangements during the course of your regularly scheduled comprehensive examination, and will request appropriate corrective action, when needed, to ensure that the arrangements satisfy safety and soundness standards. We have also updated the attached list of references to guidance on third party arrangements.

For Further Information Contact: Your Regional Office or the Supervision Policy Division of the Office of Thrift Supervision, Washington, D.C. You may access this bulletin at our web site: www.ots.treas.gov.

Thrift Bulletin 82a

Background

Savings associations increasingly rely on services provided by third parties, including affiliates and subsidiaries, to support a range of financial, operational, and marketing activities. These activities include, among other services, information technology, accounting, audit, investment management, and human resources. Third party arrangements may improve earnings, assist in managing costs, and provide expertise not available internally. At the same time, the reduced financial and operational control over third party activities poses additional risk. You should exercise appropriate due diligence before entering into third party arrangements, and maintain effective oversight and control throughout the arrangement. The assessment of the risk of these arrangements depends on the following factors:

- The significance and criticality of the activity to the association's operations.
- How well you will be able to manage, monitor, and control the risks associated with the arrangement.
- How well the third party provider manages and controls the inherent risks to your association.

Introduction

This Thrift Bulletin provides guidance on managing the risks that may arise from third party arrangements such as financial functions, operational functions, or the marketing of a third party's services and products under your name. Examples of third party arrangements addressed in this Bulletin include, but are not limited to, the following activities:

- Financial, accounting, or tax services.
- Legal services outside the normal course of business, such as services performed for a merger or acquisition, a stock issuance, or internal investigations. Legal services outside the normal course of business may also include consulting and litigation services.
- Data processing, electronic banking, network security management, and other information technology services.
- Internal audit.
- Activities that support lending operations, loan review, loan servicing operations, deposit-taking functions, funds or wire transfer, fiduciary or trust operations, compliance, brokerage services, response or loan application processes, credit underwriting for borrowers' life insurance, valuation services, or mortgage servicing.
- Asset management, human resource administration, or treasury operations.
- Physical security.
- Equipment providers or nonroutine maintenance.

- Customer call centers, telemarketing, mail houses, bill paying services, collection services, payroll processing, merchant processing activities, or forms providers.

- Real estate appraisal or credit reporting service bureaus.

- Mortgage brokerage services.

- Personnel services such as underwriting for employee health or life insurance, and retirement programs.

- Customer services, such as underwriting accident and disability insurance.

- Major construction projects, such as adding a wing to the home or branch office, or undertaking an asbestos containment project.

Using a third party to perform services and activities does not diminish your responsibility to ensure that they conduct activities and provide services in a safe and sound manner, and in compliance with applicable laws and regulations. Generally, the risk management policies that apply if you conduct an activity directly, also apply to third parties that conduct the activity on your behalf, or in your name.

OTS Requirements For All Associations

Notice

The Home Owners' Loan Act (HOLA)[1] requires that you notify OTS of arrangements with all third party providers. HOLA requires notice even in the absence of a contract, and generally applies to any service that a third party performs for you. This includes third party relationships with a foreign party[2] and is not limited to data processing services. Generally, you must give notice to your Regional Director of both domestic and foreign third party arrangements within 30 days after the earlier of:

- The date the association enters into a contract with the third party, or

- The date the third party initiates performance of the services.

The notice should provide the Regional Director with the name and address of the third party provider, the type of services the third party will perform, and a contact name at your association should OTS require additional information. Except for significant contracts with IT service providers and those with foreign providers, you do not need to provide notice of contracts you make in the normal course of business, such as routine legal services (for example, loan closings or securities filings), armored truck services, janitorial services, coffee, soft drink, or food catering services, utility services, minor outside or inside building repairs, or parking services.

[1] Section 5(d)(7)(D)(ii) of HOLA, 12 USC § 1464 (d)(7)(D)(ii), as added in 1998 by the Examination Parity and Year 2000 Readiness For Financial Institutions Act.

[2] A third party relationship with a foreign party refers to third parties whose service operations are located in a foreign country and are subject to the laws and jurisdiction of that country. This also includes U.S. providers to the extent their operations are located in or subcontracted to entities domiciled in a foreign country, and are subject to the laws and jurisdiction of that country. This definition would not include a U.S. based subsidiary of a foreign firm because its operations are subject to U.S. laws.

You do not need to provide notice of arrangements that are not significant to the overall operation or financial condition of the institution. OTS will consider a contract significant if the annual contract amount exceeds two percent of the association's total capital. OTS generally considers all arrangements with foreign service providers significant. In addition, OTS considers all information technology related outsourcing contracts that are critical to the institution's daily operations significant regardless of the contract amount.

OTS reviews notices of third party arrangements for informational purposes, and would not generally do an in-depth review until the next examination. However, if your association has a composite rating of 3, 4, or 5, or is in troubled condition, OTS may review your third party arrangements in-depth at the time you provide notice.

Recordkeeping

OTS has recordkeeping requirements that apply to thrifts and affiliates that engage third party providers, U.S. or foreign-based.[3] In general, all books and records related to the transaction of the association's business must be available to OTS for examination and audit.[4] Under 12 CFR § 562.1(b), the thrift and its affiliates must maintain, in the U.S., records comprising documents, files, and other material or property of all business transactions. This includes records provided by third party providers. Thus, a contract for third party services should contain a provision that requires the third party provider to make those records available to the thrift.

Troubled Associations

OTS has concerns about third parties providing certain services if an association becomes troubled as defined in 12 CFR § 563.555. If an association is troubled, OTS may seek control over the association's arrangements with third parties if the association is unable to manage or oversee the third party's activities. Although troubled savings associations may enter into contracts for services outside the normal course of business, they should notify the Regional Director and receive prior approval. OTS policy directs 4- and 5-rated associations to notify and receive Regional Director approval before entering into any contract outside the normal course of business. See Thrift Activities Handbook Section 310.

[3] See 12 CFR §§ 562.1(b) and 563.170 (c), which implement 12 USC § 1464 (d)(1)(B)(iii) that provides the authority of OTS in the course of examination, oversight, or for the purpose of acting on any application to receive prompt and complete access to all relevant books, records, or documents of any type. 12 CFR § 562.4(d)(2) provides requirements related to external audit reports.

[4] See 12 USC § 1464 (d)(7)(D)(i), which provides that performance by a third party is subject to regulation and examination by OTS to the same extent if performed directly by the savings association. (Certain limits affect OTS's ability to examine or require reports from a third party that is a functionally regulated entity, as provided by section 45 of the Federal Deposit Insurance Act (12 USC 1831v).) In combination with the authorities cited in footnote 3, OTS has authority to access relevant thrift records maintained by third parties.

OTS believes that using third parties to provide loan services related to subprime lending, mortgage servicing, or other arrangements [5] may create difficulties for an association to manage, or for OTS to oversee if the association becomes troubled or fails. For this reason, you should include a provision in your contract that allows you or the OTS to terminate the contract upon reasonable notice and without penalty (including contracts for IT functions) if your association becomes troubled.

Affiliates and Subsidiaries

In many cases, it is appropriate and beneficial for you to engage in business transactions with your affiliates and subsidiaries. A business relationship with an affiliate or a subsidiary should be consistent with safe and sound operations and practices.[6] Records and documentation of transactions with affiliates and subsidiaries should be readily accessible for examination and other supervisory purposes. If you use an affiliate or subsidiary to perform certain functions for you, or you perform certain functions for them, the terms and conditions of the contract should evidence an arms-length transaction, and provide for payments based on market rates. An arrangement between your association and an affiliate or subsidiary should be on terms and under circumstances that are substantially the same, or at least as favorable, to the association as those prevailing at the time for comparable transactions with a nonaffiliated third party. OTS will take appropriate supervisory action for any transaction that is abusive and detrimental to the association, or objectionable and against the association's best interests. Standards that apply to transactions between your association and an affiliate or a subsidiary also apply to any transactions between your thrift subsidiary and your affiliate.

Foreign Third Party Relationships

A thrift's use of foreign third party providers may raise unique strategic, reputation, credit, liquidity, transactional, geographic, and compliance risks that require additional oversight.[7] If you are considering establishing third party relationships with a foreign provider, you should consult with your Regional Office and carefully analyze the following factors:

---

[5] Third party activities associated with securitizations, and specifically the related servicing, require consideration of the effects a termination clause may have on the securitization products with investors. In typical securitization contracts, a Trustee controls the servicing contract and generally has discretion to terminate a servicing contract, and to select a successor servicer. This may occur if a servicer becomes troubled. To cover circumstances where a Trustee transfers a third party function to a successor party, the contract should include a provision that OTS has immediate access to and the right to examine the books and records of the successor party. OTS should also have access and the right to other information and reports (internal control or review, external audit, audit committee, board of director minutes, affiliate or subsidiary financial statements) produced by or for the successor relevant to the financial condition of a troubled association.

[6] In addition, transactions with affiliates are subject to 12 CFR § 563.41.

[7] Oversight should include consideration of Section 319 of the USA PATRIOT Act, Pub. L. No. 107-56 (October 26, 2001), 31 USC § 5318-5318A, which requires financial institutions to make information on anti-money laundering compliance by an institution or its customers available within 120 hours of a government request. The Office of Foreign Assets Control of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, organizations sponsoring terrorism, and international narcotics traffickers. For more information see OFAC website at http://www.treas.gov/ofac. Thrifts should also be aware that some foreign jurisdictions may have data privacy laws or directives that apply to information transferred from the U.S. to that foreign jurisdiction over the Internet or to information collected within the foreign jurisdiction using automated or other equipment in that jurisdiction. There are also choice of law considerations when contracting with foreign third party providers, and issues regarding standards for safeguarding customer information under § 501(b) of the Gramm-Leach-Bliley Act, 15 USC § 6801(b) and Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Transmittal No. 246).

- Your ability to perform and document adequate due diligence on the foreign provider considering the geographic location.

- Your ability to enforce contract provisions in a foreign country.

- Effects of political and economic risk that may be inherent in the foreign country on management and operations of the foreign provider.

- Ability of the foreign provider company to effectively comply with Gramm-Leach-Bliley Act (GLBA) privacy and security provisions, the USA PATRIOT Act anti-money laundering provisions, and other anti-money laundering legal obligations that apply to your association.

- Whether your surety bond covers losses, including losses from errors and omissions, that result from arrangements with the foreign provider.

- Reputation, operating history, and financial strength of the foreign provider.

While OTS does not require you to notify a third party provider that the services it performs for you are subject to OTS examination, you should include such a contract provision or other form of notification if your contract is with a foreign provider. A thrift's use of a foreign provider, and the location of critical data and processes outside U.S. territory must not compromise OTS's ability to examine a thrift's operations. Accordingly, OTS expects thrifts to establish relationships in a way that does not impede OTS's access to data or information needed to supervise the thrift or to assess the safety and soundness of the thrift's operations.

Management Responsibilities

You must retain accountability for any third party arrangement, and determine the strategic role and objectives for the arrangements. You are responsible for understanding the risks associated with third party arrangements and ensuring that effective management practices are in place. You should clearly define each party's expectations and obligations so they are enforceable. Your risk management process should include the following items:

- An assessment of risks to identify your association's needs and capabilities.

- Due diligence to identify and select a third party.

- A written contract that states the duties, obligations, contingencies, and responsibilities of the parties and ensures that third parties maintain adequate internal controls over activities.

- Policies, procedures, and controls to oversee the third party's activities and performance.

- Ongoing oversight of third party performance, including periodic assessments of costs, compliance management, acceptability of service levels, and unforeseen risks.

- Documentation regarding both the periodic assessment of a third party's performance and the due diligence that you performed to arrive at your assessment.

This Bulletin provides tools for you to use or adapt as necessary to address specific circumstances according to the individual risk profile of your association. Your risk management system for any third party arrangement should reflect the complexity of third party activities, and the overall level of risk involved. Accordingly, you should tailor your risk management based on the following items:

- Your experience with third parties, both affiliated and nonaffiliated.
- The materiality of the risks.
- Your ability to manage those risks.
- Whether the service is a one-time service or ongoing.
- The degree to which a service directly involves your customers.
- Whether the services relate solely to the association's operations, and the critical nature of those operations.

You should periodically review the arrangement, and analyze whether the targeted service levels reflect your expected improvements in operations. You may find that you need to reset target service levels as the contract progresses. You should review significant contracts annually and consider renegotiation if service levels do not meet expectations.

Risk Assessment

You should assess key risks and options for controlling third party arrangements. Factors influencing your risk assessment should include the following items:

- *The importance and criticality of the function*. A complete and realistic understanding of what the third party arrangement can accomplish includes assessing your own strategic goals, objectives, and business needs. It also involves a thorough corporate self-assessment of competencies and overall values, including an assessment of your personnel and managerial strengths and weaknesses. Consider whether the arrangement creates a potential dependency on the third party provider, and how business disruptions or problems of the provider could affect the association.
- *The nature of the activities that the third party will perform*. This includes determining the benefits, costs, and risks of the activity, as well as assessing both legal and regulatory requirements. For this assessment consider performing the following analyses :
  - — Define the requirements for the activity in terms of your current and anticipated needs.
  - — Prepare a cost/benefit analysis. Management and, if appropriate, the board of directors should approve this analysis.
  - — Determine who will make and implement critical decisions regarding the third party activity, and the effect on your association.
  - — Determine the necessary controls and reporting processes over the activity.

- Review the regulatory requirements and guidance for the business line(s) affected, including consumer protection and other compliance obligations.

- Review the regulatory requirements and guidance for the types of technologies the third party uses in providing its services.

- Determine if the third party's activities are consistent with the law, ethical standards, and your association's policies and procedures. For example, consider whether the third party protects the privacy of consumer and customer records, and has implemented appropriate information security programs. Also, consider whether you can manage conflicts of interest with affiliated third parties.

- Critically evaluate whether the third party's activities could be viewed as predatory, abusive, unfair, or deceptive to consumers, particularly if products and services offered through the association have fees, interest rates, or other terms that the third party could not otherwise offer on its own.

- Familiarize yourself with the corporate structure of the third party and understand the associated limits on liability afforded to incorporated entities, such as C-corporations, limited liability corporations (LLCs), and limited liability partnerships (LLPs). Consider any other limitations on liability imposed by a third party, such as those that often appear in standardized contracts, and whether the proposed limit is in proper proportion to the amount of loss you might experience if the third party fails to perform.

- Determine whether any third party seeks to avail itself of the benefits of a federal thrift charter, particularly with respect to the application of state and local law. Associations should not "lease" their charter out to nonthrift entities through an agreement that allows the nonthrift entity to circumvent state and local law. Some third party providers may target associations to act as delivery vehicles for certain products and services to circumvent state laws that would otherwise apply to their activities.

- Consider the provider's ability to handle your association's needs with individualized responses and timely attention without significant additional costs.

- *Availability of other parties to provide any particular function, and the costs if it becomes necessary to change the party that provides the service.* You should develop your own business continuity plan to address the potential loss of services of the third party if financial problems, insolvency, disaster, or other event that might cause a significant service disruption occurs. You should coordinate your plans with those of the third party to the extent possible to ensure that you base your plans on accurate assumptions regarding what each party should expect in the event of a disruption of services. You should keep a list of other available third parties, assessing the costs of additional due diligence, and costs to switch third parties. You should also ensure that the third party's contingency plans adequately protect your association and are compatible with your own plans.

- *An assessment of contractual obligations and requirements for both you and the third party*. As discussed in detail below, a written contract is essential for both parties to the arrangement. The contract should clearly state the rights and responsibilities of each party.

- *Your ability to perform assessments of the third party activities to evaluate consistency and third party performance on an ongoing basis.* You should determine whether you have the resources, expertise, and the will to ensure that the arrangement does not compromise your association's security, reliability, and integrity. Once you determine the services or activities third parties will perform, you are responsible for ongoing oversight, including assessment of their compliance performance.

Due Diligence in Selecting a Third Party

Regardless of the type of arrangement, selecting a competent and qualified third party with experience is essential to managing risk. The process that you use to select a third party will depend on the nature of the service. Thus, the process may be more or less formal depending on the complexity of the service, and your familiarity with prospective third parties. You should pursue, to the extent possible, a competitive bidding process to ensure that you gain a full understanding of services and features available from the various third party providers, and to obtain a realistic price point on the services.

In selecting a third party, you should critically evaluate the third party to determine its ability to meet your association's needs, and perform sufficient analysis to satisfy yourself of the following:

- The third party is competent and stable, both financially and operationally.

- The third party has the ability to provide the expected services over the life of the contract.

- The third party has made adequate representations about its activities, and presented accurate reports and materials for your evaluation.

Typically, due diligence should include analyzing the following criteria:

- *Experience in implementing and supporting the proposed activity*. You should determine the third party's competence and experience in providing the service in the particular operating environment, including the ability to provide the necessary services and supporting technology for your needs. You should identify the areas where you would have to supplement the third party's expertise to fully manage risks. Consider on-site visits, where practical, to better understand how the third party operates and supports its services. Carefully consider the drawbacks to contracting with a third party that is distant from you or in a remote geographical area. You should evaluate the third party's understanding of regulations relevant to the services they will provide.

- *Financial condition.* Consider the significance of the third party's financial condition. If the third party has an audit, analyze the financial condition of the third party using the most recent audited financial statements and annual report. Note whether the auditor's opinion is unqualified. If the third party is a public company, you should analyze other indicators, such as publicly traded bond ratings, if available. If a third party provider does not have audited financial statements, you should analyze the company's most recent and year-end balance sheet and income statement. Consider comparing the most recent year-end financial statements to the previous year-end statements to determine whether or not any positive or negative trends are apparent regarding the soundness of the company's financial condition. You may find the financial condition of privately held providers, those who are start-ups, or those with atypical balance sheets (intangible assets and goodwill) difficult to assess. In those instances, consider treating the third party provider as a borrower, and look to factors relevant to your

association's loan standards. If a provider, such as a small provider, does not have audited financial statements, you may want to consider requesting its tax return, which may provide basic information as to its asset size and income. You may also want to consider the provider's reputation, credit history, and track record in providing the necessary services, especially to other financial institutions, as well as its market share. As with any due diligence process, you should inquire as to pending or threatened litigation or legal claims that could affect the provider's financial stability. In general, analyze the available information to the best of your ability. Overall, a standard guideline might be to ask yourself whether you would make a loan to this company. However, when financial information is unavailable, you should consider this lack of information as a risk in your overall assessment of the third party.

- *Business reputation, complaints, and litigation past and pending.* Consider how long the third party has been in business, and the third party's market share for a given service, and whether it has fluctuated. You should determine who serves as the third party's significant principals and their relationship to the third party's operations, if any. You should also contact references and other user groups to learn about the third party's reputation and past performance. You should review year-end financial statements for litigation disclosures, and ask third party management about past litigation, and if any litigation is pending.

- *Staff competence, qualifications, and training*. You should evaluate key personnel that the third party would assign to support the association.

- *Internal control environment*. You should determine the third party's standards, policies, and procedures relating to internal control, maintenance of records, privacy protection, facilities management, security, contingency plans, and employee background checks. Consider reviewing audit reports of the third party, such as reports on the internal audit function or internal control evaluations and assessments. If a service organization provides services that are part of an association's information technology system, such audit reports may include reports prepared by an independent auditor in accordance with AICPA Statement on Auditing Standards (SAS) No. 70, "Service Organizations," (AU 324). These reports may provide you additional information regarding the adequacy of the third party's internal controls, policies and procedures, and security safeguards.

- *Information and reporting systems*. Consider whether you will have to provide additional systems or perform additional work yourself to enable the third party to perform the proposed services. You should determine if the third party has adequate resources to protect association resources as well as detect and respond to problems. Also, you should evaluate whether you will have complete and timely access to information maintained by the third party.

- *Contingency and recovery plans*. You should evaluate the third party's ability to respond to service disruptions.

- *Subcontractor reliance*. You should assess the third party's use of other parties or partners to support the third party's activities. You should determine whether the third party understands that it is its responsibility to ensure that its subcontractors are in compliance with all regulatory requirements including the GLBA and the USA PATRIOT Act, as it relates to the work being done for the association, and the security of and handling of confidential nonpublic information that the association may provide.

- *Insurance coverage*. You should ensure that the third party has both fidelity bond coverage to insure against losses attributable to dishonest acts, and liability coverage for losses attributable to negligent acts in an amount that you determine to be safe and sound given the potential exposure to risk through the third party arrangement. Also, you should review insurance covering fire, loss of data, and protection of documents.

Contract Issues

A contract should act as a map to the relationship and define its structure. You should obtain a written contract for all services, but particularly for significant or material services critical to your operations. The written contract between you and the third party should clearly specify, at a level of detail commensurate with the scope and risks of the third party activity, all relevant terms, conditions, responsibilities, and liabilities of both parties. When contracting for the services of a third party, be aware that OTS generally has authority to examine a third party's activities, and where applicable, may pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by you or your third party. OTS's authority to examine third parties is not a substitute for your responsibilities for due diligence, maintenance of controls, and ongoing oversight.

The list below provides some of the important things to consider when contracting with third parties. The list is not all-inclusive, and you may need to evaluate other considerations based on your unique circumstances. Depending on cost, risk, and criticality of the function, you should consider having qualified legal counsel review the contract.

A contract should typically include the following terms:

- The scope of the arrangement, including types of service and activities, performance standards, warranties, and penalties for lack of performance.

  — Identify the frequency, content, response time, and format of the third party's service. Where possible, specify performance measures to define the expectations and responsibilities for both parties. The contract should also discuss the frequency and type of reports you expect to receive. It is likely that you will get only what you ask for in terms of reports and analysis from third parties.

  — Detail the third party's conduct while on your premises, and describe the terms governing the third party's use of your space, personnel, and equipment.

  — Address a third party's use of subcontractors or other entities. You should require that the third party provide you notice of its use of subcontractors, and that you give approval.

  — Address how to handle customer complaints, if applicable. You should implement procedures to ensure that either you, or the third party under your oversight, appropriately address the complaints. Monitor complaint activity, the substance of the complaints, and responses.

  — Specify the period covered by the contract and the delivery point for goods and services.

  — Review liability and recourse arrangements, if any, in the contract. Check to see if the contract imposes on your association any potential liabilities to carry out an activity should the third party fail to perform.

- Insurance, disaster recovery capabilities, and other contingency measures that the third party maintains.

  — Include specific provisions addressing insurance coverage, and require periodic verification that policies are in force.

  — Ensure that the contract does not contain any provisions that would excuse the provider from implementing its contingency plans.

  — Include specific provisions for business recovery periods that meet your business requirements.

  — Address the third party's maintenance of disaster recovery and contingency plans including backup and record protection.

  — Consider materiality thresholds and procedures for the third party to use to notify you if there are service disruptions, security breaches, or other events that pose a material risk to your association.

  — Consider requiring the third party to notify you in the event of financial difficulty, material change in strategic goals, and significant staffing changes, all of which may affect service.

  — Consider the third party responsibility for "Act of God" events.

- Ownership and access.

  — State the third party's permitted use, if any, of your data, hardware and software, system documentation, and intellectual property, such as your name, logo, trademark, and copyrighted material.

  — Clarify licensing issues, particularly in the case of software licensed to you that the third party may use. Ensure that you have access to source codes, and documentation of programming and systems.

  — Indicate whether any records generated by the third party are the property of the association.

- Provisions for your access to external audits, internal control reports, if available, or other reviews of and reports on the third party's operations and financial condition.

  — Include the types and frequency of the audit reports you expect to receive. (For example, financial and internal control reviews.) Internal audit reports or other independent third party reviews (including SAS 70 reports) and work papers regarding the third party provider's internal audit function must be available to OTS examiners upon request.

  — Ensure that the third party has an effective internal audit function in place. If not, consider including a provision that the third party provider have an independent party review the provider's internal audit function, or include a provision that you will perform the review. A third party provider may reserve the right to use its own internal audit staff to conduct a review of its internal controls or a review of the functions it provides for you. Consider whether to accept internal audits and reviews conducted by the third party provider's own internal audit staff or whether you prefer an independent party to perform the work (for example, SAS 70 reviews).

— You may also consider including a provision that the provider obtain an annual external audit performed by an independent external auditor if the third party's activities, based on the nature, complexity, and cost of the services are significant and critical to your operations. This may assist you in determining the provider's financial condition.

— For a third party subject to SEC or other independence guidance, such as that issued by the AICPA, you should clarify that the third party will not perform management functions, make management decisions, or act in a capacity equivalent to that of an employee of the association.

- Compliance with any applicable regulatory requirements, and access to information and operations by OTS and other regulators.

  — You should give the third party provider notice that its performance of services on your behalf is subject to OTS examination and oversight. If the contract is with a foreign service provider the notice should be in the form of a letter or contract clause. OTS has authority for examination and oversight under HOLA (see footnote 1). Your notice should specify that OTS generally has the authority to examine and regulate the third party's function or operations on your behalf, and to require reports, as if you performed the function or operation yourself on your own premises. You should clarify that this includes, but is not limited to, OTS authority to examine and regulate a third party or its successor to evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, and compliance with other applicable laws.

  — State that the third party provider will comply with applicable law, and not take actions that would lead to violations of law by the thrift.

  — You should include a termination provision for any third party arrangement when OTS requires termination, such as when your association becomes troubled or in the event the OTS formally objects to the arrangement. The termination provision should be effective upon reasonable notice and without penalty.

  — Specify responsibility for applicable taxes, state and federal.

- Provisions for handling disputes, contract changes, contract default and termination, assignment of the contract, and indemnification.

  — Specify liability for delayed or erroneous transactions, and other potential risks.

  — Include a termination provision for change in control, merger or acquisition, convenience, substantial increase in cost, repeated failure to meet service standards, failure to provide critical services and required notices, failure to prevent violations of law or unfair and deceptive practices, bankruptcy, company closure, and insolvency. Consider whether the contract allows you to terminate the relationship without prohibitive expense. Also consider reserving your right to retain other third parties.

  — In instances where the third party may seek to terminate its contract to provide services for you, ensure that your contract contains the following provisions:

- That the third party provides you timely written notice of the intent to terminate. The contract should state termination and notification requirements.

- That the terminating party provides you with a reasonable advance notice period before terminating its services and provides adequate time frames to allow for the orderly conversion to another provider. You should determine the amount of time you will need to safely convert to another third party provider.

- That the terminating party will cooperate in effecting an accurate and timely return of your association's information and data, or transfer or conversion of your association's data and records to a replacement third party provider.

- Clearly state the obligations of the third party provider for costs and services associated with a transition.

— Require notification of material changes in insurance coverage.

— Consider use of alternative dispute resolution (ADR) procedures.

- Costs and compensation.

  — Fully describe the fees and formulas for calculations of charges for the third party's activities. Also, address fees and charges for changes in or additions to services.

  — Indicate who is responsible for payment of legal, audit, and any other fees associated with the activity. Address who is responsible for purchasing and maintaining hardware and software associated with the services.

  — Clearly state invoicing and payment procedures.

  — Ensure that you have established a fee structure at market rates and terms.

  — Consider conditions where the cost structure may change, and consider setting a ceiling on cost increases.

  — Contracts may offer bonuses for exceptional performance and penalties for poor performance. Any such bonus or penalty should align the interests of the third party provider to the interests of your association.

- Confidentiality and security.

  — Prohibit the third party and its agents from using or disclosing any of your information, except as necessary to provide the contracted services.

  — Require the third party to disclose breaches in security resulting in unauthorized intrusions that may materially affect you or your customers, and address the powers of each party to change security procedures.

In general, contracts need to be flexible, and therefore, should not be long-term (over five years). It is difficult to foresee and contract for every possible contingency that may arise. Also, business needs change or the market may evolve in unexpected directions. For these reasons, OTS discourages long-term contracts. Shorter contracts may provide more flexibility to meet the challenges of a changing environment.

Policies, Procedures, and Internal Control

Third Party Provider

The third party provider should have an effective internal audit function in place. It should implement internal control policies and procedures, including those for data security and contingency capabilities, and other operational controls that are analogous to those that you would perform if you performed the activity internally. When appropriate, an independent third party should review the adequacy of the third party provider's system of internal control.

Management

You are responsible for having an effective system of internal control and an effective internal audit function that supports your association's internal control policies and procedures for third party oversight. Your system of internal control and the internal audit function should provide you with reasonable assurance that a third party's activities and services are valid, complete, properly authorized, and accurate. An audit provides the independent review necessary to ensure that the third party is implementing the process in a way that is consistent with your objectives. You should have reasonable assurance that your system of internal control and internal audit function prevents or detects the following intentional or inadvertent third party actions:

- Creating significant inaccurate, incomplete, or unauthorized transactions.
- Causing significant deficiencies in the safeguarding of assets.
- Producing unreliable financial and regulatory reports.
- Deviating from laws, regulations, or the association's policies.

You may want to ensure that you have the right to audit or review the third party provider (and its subcontractors) as needed to monitor performance under the contract. At a minimum, you should ensure that the third party is having periodic independent internal reviews at an interval and scope consistent with its functions. Whether you conduct a review of the third party provider yourself or accept the work of another reviewer, you should ensure that an independent review takes place. You should review reports on the third party provider's system of internal control and internal audit function, and make sure that the provider addresses any weaknesses or concerns its own staff or an independent party raises.

Ongoing Oversight of Third Parties

You should review the operational and financial performance of critical third parties on an ongoing basis to ensure that the third party meets and can continue to meet the terms of the third party arrangement. In general, this should include monitoring the third party's financial condition, its controls, and the quality of its services and support. Monitoring should include an audit, or control review, of the function, according to a scope and frequency appropriate for the particular function. In addition, OTS expects the board of directors to annually review significant third party arrangements. OTS requires boards of direc-

tors, or an appropriate committee of the board of directors, to approve, as well as to oversee the development, implementation, and maintenance of the institution's information security program. (See Appendix B to 12 CFR Part 570.)

The degree of oversight activities will vary depending upon the nature of the services. Consider if the third party conducts its own similar oversight activities for any of its significant subcontractors, and whether you may need to perform such oversight of subcontractors.

You should ensure you dedicate sufficient staff with the necessary expertise to oversee the third party. Your staff should have sufficient training and expertise to comprehensively review the third party's performance, financial status, and risk controls. OTS expects you to document your oversight program, and obtain certain board of directors' approvals. OTS also expects you to maintain adequate reports and records to enable examiners to effectively and fully review your operations, even if you use a third party to perform a function or provide a service.

In assessing the third party's performance, include, as appropriate, the following activities:

Monitoring Financial Condition and Operations:

- Annually evaluate the third party's financial condition. Perform evaluations more frequently if risk is high, or moderate and increasing. The analysis should be as comprehensive as an ongoing credit analysis of one of your borrowers.

- Require the third party to submit audited financial statements when the nature, complexity, cost, and criticality of the activities are significant to the operations of your institution.

- If applicable, ensure that the third party is meeting its financial obligations to subcontractors in a timely manner.

- Review the adequacy of the third party's insurance coverage, note material changes, and verify that the policy (or policies) is in force.

- If appropriate, consider comparing actual earnings and costs with projections.

- Review audit reports. For example, review reports prepared in accordance with SAS No. 70, external audit reports, reports on internal control, security reviews, and examination reports, if available.

- Follow up on any deficiencies noted.

Monitoring Controls:

- Review the third party's policies relating to internal controls and security to ensure that they continue to meet your minimum guidelines and contract requirements.

- Ensure that the third party meets your requirements under GLBA if it handles nonpublic customer information.

- Perform on-site quality assurance reviews, targeting adherence to specified policies and procedures, where practicable and necessary.

- Sponsor coordinated audits and reviews with user groups, as applicable.

- Review whether the third party renders services in a manner that maintains your compliance with the Bank Secrecy Act, fair lending, GLBA, and other consumer protection laws and regulations, as applicable.

- Review the third party's business resumption contingency planning and testing to ensure that the third party can restore all services in an acceptable time. Review testing results to ensure that recovery times meet your requirements. For critical services, annual or more frequent tests of the contingency plan are typical.

- Monitor changes in key personnel the third party allocates to your activities.

Assessing Quality of Service and Support:

- By regularly reviewing reports and documenting the third party's performance relative to the contractual agreement, determine whether the third party is meeting the contract's terms and conditions, and whether you need to make any revisions to the agreement.

- Ensure that you have complete and immediate access to information critical to your operations that the third party controls.

- Document and follow-up on performance problems in a timely manner.

- Evaluate the third party's ongoing ability to support and enhance your strategic plan.

- Review customer complaints regarding the third party's products and services, and monitor the resolution of these complaints.

- Where appropriate, consider administering mystery shopper, customer callback, or customer satisfaction programs.

- Periodically meet with the contract parties to discuss performance and operational issues.

- Maintain documents and records regarding contract compliance, revisions, and dispute resolution. This should include reviewing invoices to assure proper charges for services.

Documentation:

- Document your procedures used for due diligence.

- Include information on the number of bids received.

- Maintain a list of all third party providers and indicate if they are significant or critical. This would include those you spend a substantial amount of money on, or those you deem critical to your association's operation.

- Maintain a policy that your board of directors, or an appropriate committee of the board of directors, approves and documents your process for entering into significant third party arrangements.

- Document in the board of director's minutes your review of business plans for significant new lines of business or products. The minutes should reflect your planning process, decision making, and, in the case of significant contracts, your due diligence in selecting third party providers.

- Retain and present to management and, when appropriate, to the board of directors, or an appropriate committee of the board of directors, regular risk management and performance reports received from third parties for significant contracts. For example, audit reports, security reviews, cost reports, and reports indicating compliance with the contract.

- Maintain valid, current, and complete contracts.

- Prepare and retain regular reports for management and, when appropriate, for the board of directors, or an appropriate committee of the board of directors, of the results of the ongoing oversight activities for significant third party arrangements.

OTS Supervision

OTS's supervisory approach to any third party provider arrangement, including one with foreign third party providers, will emphasize your responsibilities to:

- Manage risks appropriately.

- Conduct adequate due diligence.

- Comply with applicable laws.

- Ensure access to critical information with respect to the third party's activities.

In assessing your management of the third party arrangement, OTS examiners may want to review the following areas:

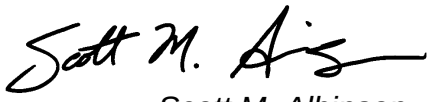
- Business plans for significant new lines of business or products using third parties or newly out-sourced functions.

- Results of due-diligence reviews.

- Contracts.

- Information provided to your management and board of directors reflecting results of ongoing monitoring activities.

OTS will focus on the results of your due diligence, risk assessment, and ongoing oversight program. If OTS finds any of these risk management processes deficient, OTS may examine the third party, require you to take the necessary steps to strengthen risk management controls, or terminate the outsourced arrangement.



—Scott M. Albinson
Managing Director
Examinations, Supervision, and Consumer Protection

REFERENCES

More guidance about outsourcing arrangements and third party relationships can be found in the following documents:

Issuance	Subject	Applicability to Outsourcing
Statutes 12 USC 1464(d)(7)	Home Owners' Loan Act (HOLA), as added in 1998 by service provider examination provisions of the Examination Parity and Year 2000 Readiness for Financial Institutions Act	Establishes the OTS's authority to examine and require reports from vendors providing services to savings institutions and rules for contracts between depository institutions and parties providing goods, products, and services.
Public Law 106-102 (15 U.S.C. 6801, et. seq.)	Gramm-Leach-Bliley Act (11/12/1999)	Places limitations on OTS's authority to examine and require reports from functionally regulated entities. Title V provides rules regarding privacy and security.
Public Law 107-56	USA Patriot Act (10/26/2001)	Provides, among other things related to September 11th, anti-money laundering provisions.
OTS Regulations **12 CFR**		
Part 555 (2002)	Electronic Operations	Establishes authority and requirements for savings associations to conduct electronic operations.
563.191 (2002)	Bonds for Agents	Rules for fidelity bonds for agents appointed by a savings association.
563.41 (2003)	Transactions with Affiliates	Restrictions on transactions between a savings association and an affiliate.
Part 570 (2002)	Appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information	Rules to develop and implement a customer information security program.
Part 573 (2002)	Privacy of Consumer Financial Information	Obligation of a financial institution to inform the consumer of its information-sharing practices, which may include outside vendors.

CEO Letters No. 59	Risk Management Client Server Systems (10/24/1996)	Alerts institutions to risks associated with the client/server computing environment.
No. 70	Statement on Retail On-Line Personal Computer Banking (6/23/1997)	Describes risks involving the use of a PC for retail purposes.
No. 79	FFIEC Guidance Concerning Due Diligence in Connection with Service Providers and Software Vendors as well as Guidance Concerning the Year 2000 Impact on Customers (3/29/1998)	Provides extensive guidance for establishing a due diligence process to determine a vendor's ability to become Year 2000 ready. It includes testing approaches and schedules, as well as methods to evaluate performance contingency plans.
No. 88	FFIEC Guidance Concerning Contingency Planning and Customer Awareness (6/18/1998)	Provides guidance on Year 2000 vendor management.
No. 90	Interagency Guidelines on Electronic Financial Services and Consumer Compliance (7/23/1998)	Discusses regulatory issues, and implications of electronic technologies for consumers.
No. 109	Transactional Web Sites (6/10/1999)	Provides notice requirements for establishing a transactional web site.
No. 129	Privacy Preparedness Check-up (9/29/2000)	Provides some guidance regarding application of customer privacy policies to vendors.
No. 132	Payday Lending (11/27/2000)	Some discussion of the various risks with vendors involving payday lending outsourcing.
No. 139	Identity Theft and Pretext Calling (5/04/2001) (Includes Federal Register Notice Vol. 66, February 1, 2001 at 8618-8619, and 8623-8624)	Provides guidance for contract provisions and oversight mechanisms to protect customer information, maintained or processed by outside vendors. Also discusses the institution's responsibilities.
No. 143	Authentication in an Electronic Banking Environment (8/09/2001)	Discusses evaluating and authenticating systems and practices of the electronic banking environment.
No. 201	FFIEC Information Technology Handbook, Outsourcing Technology Services (7/15/04)	Provides guidance for managing risk in connection with information technology (IT) services provided by outside firms.

Thrift Bulletin (TB)		
TB 11-1	Purchased Software Evaluation Guidelines (4/20/1989)	Discusses risks in purchasing vendor software and provides guidelines to evaluate the purchase.
TB 23-2	Interagency Statement on Retail Sales of Nondeposit Investment Products (2/22/1994)	Discusses guidance for financial institutions that provide retail nondeposit investment products to customers through arrangements with third parties.
TB 23-3	Joint Interpretations of the Interagency Statement on Retail Sales of Nondeposit Investment Products (10/13/1995)	Clarifies aspects of TB 23-2 that relate to third party sales of retail nondeposit investment products.
TB 44	Interagency Statement on EDP Service Contracts (2/07/1990)	Alerts institutions to risks in contracting EDP Services
TB 81	Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (3/17/2003)	Discusses internal audit control procedures and outsourcing internal audit work. Replaces CEO Memo No. 77 (12/30/1997).
TB 83	Interagency Guidance on Weblinking: Identifying Risks and Risk Management Techniques (4/23/03)	Provides guidance to institutions that subcontract with a service provider to create, arrange, and manage their websites, including weblinks.
Thrift Activities Regulatory Handbook (TAH)		
TAH 310	Oversight by the Board of Directors	Provides a reminder that troubled institutions may not enter into third party contracts outside the normal course of business without pre-approval.
TAH 320	Meetings with the Board of Directors	Discusses responsibilities of directors in general. These responsibilities would apply to outsourcing arrangement oversight.
TAH 330	Management Assessment	Discusses management's role in outsourcing arrangements, and provides a general discussion on internal control. Includes a discussion of requisite knowledge, skills, and abilities for management, which are applicable to overseeing outsourcing arrangements.
TAH 340	Internal Control	Describes a safety and soundness examination program to evaluate internal controls, with some discussion on outsourcing.

Thrift Activities Regulatory Handbook (cont.)		
TAH 341	Technology Risk Controls	Describes a safety and soundness examination program to evaluate technology risk controls relevant to outsourcing. Discusses outsourcing and independent service providers, including, vendor management risk, management oversight, and disaster recover plans for outsourced systems.
TAH 355	Internal Audit	Includes section with specific emphasis and detail on outsourcing.
TAH 380	Transactions With Affiliates and Insiders	Discusses requirements when associations engage in business transactions with affiliates and insiders, which may occur in some outsourcing arrangements.
TAH 710	Networking Arrangements	Provides guidance on third party arrangements to establish a brokerage dealership. Discusses affiliate and nonaffiliate third party arrangements.