Introduction to Audits

This section provides guidelines to evaluate a trust department's audit program and to evaluate the work performed by internal and external auditors. Many of the considerations used to evaluate a trust department's audit program are the same as those used to evaluate the savings association's overall audit, although a separate trust department audit should be conducted. Due to the fact that the trust department may be audited at the same time as the savings association itself, in some regions examiners (other than trust and asset management examiners) may evaluate such matters as the auditor's independence and competence for the institution as a whole. In these cases, the examiner evaluation should separately consider the independence and competence of the auditors with regards to the trust department.

The primary objective of the audit function in the trust department is to detect errors and irregularities and ascertain the effectiveness of the policies and procedures used for the administration of accounts, safeguarding of assets and the accurate recording of transactions.

12 CFR §550.440 requires that a savings association must conduct a suitable audit of its significant fiduciary activities. The regulation permits the savings association to conduct these audits on either an *annual* basis or on a *continuous* basis. If the institution chooses to use an annual audit system it must "arrange for a suitable audit of all significant fiduciary activities at least once during each calendar year" (§440(a)). On the other hand, if the savings association adopts a continuous audit system, it must "arrange for a discrete audit of each significant fiduciary activity at an interval commensurate with the nature and risk of that activity" (§440(b)). Therefore, under this type of audit system, some fiduciary activities may receive audits at intervals greater or less than one year, as deemed appropriate for the risks associated with that activity. For institutions on a continuous audit system, examiners should ensure that a risk assessment has been made for all significant fiduciary activities and that those activities reviewed less often than annually have been determined to be low risk.

Independent audits enhance the probability that conditions that could adversely affect the savings association, OTS or the public will be detected. The audit process also subjects the policies, procedures, records and the internal controls of each institution to periodic review.

Examiners should evaluate a savings association's audit program for its trust department based on a review and evaluation of the competence and independence of the audit staff and the adequacy and effectiveness of the audit program. Areas that would normally be subject to criticism include the absence of an audit function; an inadequate audit program; instances where audit staff is restricted from full access to records or otherwise lacks independence; lack of competence; instances in which the audit function does not report directly to the board of directors (or an appropriately designated committee); and instances where the board or its designated committee is not properly established or initiating necessary corrective action based on audit findings.

Materials that pertain to overall audit policies and standards are noted in more detail in sections 350 and 355 of the Thrift Activities Handbook. Only a brief summary of those materials is presented in this handbook chapter.

Audit Committee

12 CFR §550.470 provides savings associations with guidance as to the composition of the board of director's fiduciary audit committee. Under the regulation, a fiduciary audit committee directs the conduct of the audit. The composition of the committee may consist of a committee of the savings association directors, an audit committee of an affiliate or the entire institution's board of directors. However, the regulation places the following two restrictions on who may serve on the committee:

- savings association officers or officers of an affiliate who participate significantly in administering fiduciary activities may not serve on the committee; and
- a majority of the members of the audit committee may not serve on any board committee responsible for the savings association's administration of its fiduciary activities.

Results of fiduciary audits (including significant actions taken as a result of the audit) must be reported in the minutes of the board of directors.

Trust Department Audit Objectives

The objectives of a trust department audit should be:

- to appraise the soundness and adequacy of accounting, operating and administrative controls and procedures designed to insure prompt, efficient and accurate recording of transactions and safekeeping of assets.
- to determine the degree of compliance with applicable law as well as the institution's policies, practices and procedures.
- to keep the board of directors and management informed of the institution's condition and make recommendations for improvement.
- to evaluate the institution's exposure to liability if the institution fails to fulfill its duties and responsibilities to trust and asset management accounts.
- to detect and prevent irregularities such as errors and fraud.
- to determine the quality of account administration.
- to verify that fee income from trust and asset management activities is recognized properly on the savings association's financial statements.

Examiners should ensure the trust audit function is effective in evaluating the department's internal controls and is of sufficient scope and coverage to protect the interests of trust and asset management accounts and the institution. Examiners should also ensure that the auditors review for compliance with applicable law. The review and evaluation of the audit function should be a key element in determining the scope of the trust and asset management examination. The examiner should generally not duplicate satisfactorily performed audit procedures, particularly those involving verification activities.

Audit reports should provide the examiner with information pertinent to the trust and asset management examination, such as areas where weaknesses were noted and areas where the examiner should determine whether management appropriately corrected cited deficiencies. If the examiner determines that audits have not been performed or that audit work is considered to be of limited value, the examiner should expand the

scope of the trust and asset management examination. In those instances, the audit or audit program and lack of board oversight should be criticized.

Internal and External Audits

In order to satisfy the requirements of §550.460, internal or external auditors, or a combination of both may perform a trust department audit, and should be responsible only to the savings association's board of directors. The form of audit developed and the personnel employed to conduct it will be primarily dependent upon the size and complexity of the trust and asset management activities. The scope and objectives of an external audit may differ somewhat from those of an internal audit. An external audit is generally aimed at enabling the accountant to express an opinion on the fair presentation of financial statements in conformity with generally accepted accounting principles. To that end, the audit requirements subject the accounting policies, procedures, records and the internal controls of each institution to periodic, independent critical review and evaluation and typically cover only a specified historical period.

On the other hand, the internal audit function has a number of objectives, including the detection of errors; determination of compliance with an institution's policies, procedures and applicable law; and evaluation of the soundness and adequacy of an savings association's system of internal controls. Internal auditors may also play a role in the formation and revision of policies and procedures.

Actual practice may blur the distinctions between an internal and external audit. For example, internal and external auditors may work together on the same audit and set the audit scope and assign each auditor an area of responsibility or they may work side by side. Any distinction between internal and external audits is therefore relevant only to the extent that it impacts the quality and effectiveness of a savings association's overall audit program.

If the trust department is audited internally, the examiner should take the opportunity to review the auditor's programs, workpapers and reports as part of the overall examination process. However, if the department is audited externally the opportunity to review programs and workpapers may not always be feasible. In order to adequately assess the work performed by the external auditor, and to address the matters discussed in the preceding paragraph, the external audit report should provide adequate details concerning the areas audited (testing for receipt of income from investments, allocations of income and principal cash, etc.). A statement to the effect that "all applicable audit procedures were performed in compliance with PA-7a," without further elaboration, would not be acceptable. Examiners should encourage management to contact the external auditor and enable examiner access to audit programs and workpapers.

Competence and Independence

(The Thrift Activities Handbook contains detailed information on the competence and independence of auditors; only a brief summary is presented here.)

Two of the major considerations in evaluating the work of auditors are their competence and independence. This evaluation is the same as it would be for evaluating any audit or auditor; the fact that it is a trust department audit makes no difference. Thus, when a trust and asset management examination is being conducted as part of an examination of the entire savings association, an examiner (other than a trust and asset management examiner) may perform the audit evaluation of the trust department.

The very nature of an internal audit requires that it be independent. Only by being independent can the audit function fulfill its purpose of serving as a managerial control within an organization, i.e. to measure and

evaluate the effectiveness of operations and controls. To be independent means that the audit function should report only to the board of directors or its designated committee. The auditor should have full and free access to all books and records. Auditors should not audit any activity for which they are responsible on a daily basis; for example, auditors should not evaluate vault procedures if they are the vault custodians.

The size and complexity of a savings association's trust and asset management activities as well as the emphasis placed on the audit function by the board of directors will account for variations in the responsibilities and qualifications of internal auditors. In considering the qualifications of the audit staff, it is necessary to review the educational and experience qualifications required by the savings association for a position in the audit department and any available training. The trust department auditor must possess sufficient education and training to fully understand trust and asset management administration, investment practices and trust department operations. If a savings association has a small trust department, it may not always be feasible for its auditor to have trust department auditing experience. However, in those cases the auditor should participate in courses or programs sponsored by industry groups dealing with trust department audits and should review current literature on trust department auditing.

Conclusions in regard to the auditor's competence should be derived from a review of the audit program, training and the quality of reports. Indicators of the competence of the internal auditor include the quality of the work performed and the ability to communicate the results to the board.

The independence of the external audit function is similarly critical to the satisfactory performance of audit activities: external auditors must be independent of those for whom they work. The AICPA and OTS have promulgated standards of independence. OTS provides that a public accountant will not be considered independent if, among other things, the accountant or his or her firm has any direct or material financial interest in the savings association. A financial interest is defined as the CPA being connected with the savings association, subsidiary or affiliate as an officer or director; being the beneficial owner of any shares of stock of the savings association; or having any conflict of interest by reason of business or personal relationships with management or other individuals. Absent unusual circumstances, it should not be necessary to review the independence of the external auditor.

Qualified public accountants are required to perform their work according to generally accepted auditing standards. Absent unusual circumstances, it should not be necessary to review the qualifications of the external auditor. Where a review is considered necessary, the above standards relating to specialized work experience would be appropriate.

Audit Program

A savings association should develop a written audit program approved by its board or audit committee. The program should be tailored to the institution's trust and asset management activities; the risks associated with those activities; the experience level of the audit staff; and define an acceptable scope and frequency schedule for the audit. The scope and frequency of the audit testing should be dependent on the degree of risk that the trust and asset management activities pose to the savings association. Riskier activities should be audited more frequently, while those activities posing a minimal risk to the savings association may be tested on a more infrequent basis.

In the case of an external audit, a written program usually consists of having the external auditor submit an engagement letter to the directors prior to beginning their work. Engagement letters typically include the scope of the audit, the time period for the audit, and the reports expected to be rendered. The auditor may also provide a summary of procedures to be used, for example, in the verification of account assets. In the

case of an internal audit, a written program usually consists of a board resolution or an adopted procedure similar to an engagement letter.

The scope of the audit program must be broad enough to include all significant operations and functions of the trust department; however, its focus should be on the activities or operations of the trust department that have been associated with a high level of risk.

To illustrate, the scope of the audit program should consider the:

- past performance or results of past audits.
- organizational structure of the trust department.
- size and complexity of trust and asset management activities (dollar value of assets, level of discretionary accounts, complexity of assets, etc.).
- nature and extent of comments in OTS trust and asset management examination reports.
- individual factors, such as: effectiveness of internal controls, strength and integrity of trust department accounting, recordkeeping and other systems.
- nature and extent of insurance coverage.

Regulatory requirements for the scope of external and internal audits include, among other things, that:

- the audit be made in accordance with generally accepted auditing standards.
- the auditor be generally familiar with applicable law such as appropriate federal and state statutes and OTS regulations (e.g., 12 CFR §550).
- the audit incorporate all procedures necessary to satisfy the auditor that fiduciary activities are being administered in accordance with applicable law, fiduciary assets are being properly safeguarded and transactions are being recorded in appropriate accounts in a timely manner.

Audit Controls

The audit of a trust department can be divided into three main areas: compliance, physical control and activity control. Compliance consists of the prompt and complete fulfillment of all duties required by applicable law and management policies. Physical control includes the physical security of assets for which the trust department is responsible. Activity control includes the complete, accurate and timely recording of all individual account and departmental transactions.

The auditor's primary responsibility in auditing internal controls is to determine that such controls are in place, that the controls address all of the trust department's duties regarding trust and asset management accounts and that the department is in compliance with the internal controls. In terms of physical controls, the audit procedures employed will be determined at least, in part, by the extent to which the department's systems are automated or are otherwise controlled internally. For example, the auditor may perform more actual verification procedures in an automated department so as to determine whether the reconciliation of balances and statements are being properly performed by the internal accounting system, whereas in a nonautomated department the auditor may perform more actual reconciliation of account balances and controls.

An audit should include a review of the organizations that provide services to the department. Such a review will most likely be conducted by reviewing the service provider's own audit report. Such reports are rendered by the servicer pursuant to Statement on Accounting Standards (SAS) 70, which should discuss the control structure in place for trust department service providers, such as data processing servicers and securities custodians. The institution's auditors most likely will be preparing similar SAS 70 reports for use by other auditors, such as a plan sponsor's auditor and also for the trust department's common and collective investment funds.

Audits of Common Procedures and Administrative Audits

An effective trust department audit should include tests of systems and procedures that are common to the management of all or most accounts being administered, as well as tests of activity in individual accounts. Functions that are normally tested are the opening and closing of accounts; processing of assets into and out of the vault; fee charges and payments; and processing of asset purchases and sales.

Testing of individual account activity is referred to as an "administrative audit." In performing administrative audits, the auditor should perform sufficiently detailed tests to obtain reasonable assurance that activities and transactions within the various types of accounts are being conducted properly. A representative sample of accounts should therefore be selected for testing of individual transactions. The approach taken in a particular audit program will determine which functions are tested as part of common procedures and which functions are tested individually as part of an administrative audit. For example, a test of uninvested cash could be performed as a common procedure by obtaining a listing of all such cash or it could be performed as an individual account procedure.

In reviewing the savings association's internal audit program, the examiner should expect to find the following minimum functions being performed:

- Review of trust department committee minutes
- Balance and proof of subsidiary ledgers to general ledger
- Review of broker confirmations
- Spot-check and tracing of transactions for accuracy and validity
- Verification of commission and fee calculations
- Assessment of compliance with applicable law
- Evaluation of internal controls
- An administrative review of selected accounts comprising:
    - The trust agreement, other governing documents and court orders
    - Administrative actions (in compliance with above)
    - Income postings
    - Discretionary distributions
    - Principal invasions (including approvals therefore)
    - Investments in accordance with account objectives and department policy
    - Account documentation

- Consultation with, and approvals by, cofiduciaries

Audit Records and Reports

In order to have a sound basis upon which to evaluate the adequacy of the internal audit program, the audit workpapers must document the work performed by the auditor. Workpapers should contain audit work programs and analysis that clearly indicate the procedures performed, the extent of testing and the basis for the conclusions reached. In addition, the content of the workpapers is one indicator of an auditor's competence and adherence to professional standards. An analysis of the reporting process followed by the auditor and of the findings and recommendations in the audit reports is important in determining the auditor's duties and the independence of the audit function.

Audit reports should be submitted as soon as practicable after completion of the audit. Reports should be sent to those officials who have both the responsibility and the authority to implement the suggested changes. Management's prompt and effective response to the auditor's recommendations is essential to the effectiveness of the audit program. The examiner should determine not only what was contained in the auditor's reports but also the timeliness and content of management's response. The examiner should expect to see either corrective action taken in response to the audit findings or reasons for nonimplementation.

Risk Based Audits

Risk based audit programs are a relatively recent development in the trust and asset management activities arena and are being more widely adopted by trust departments. The primary objectives for implementing a risk-based audit program are to improve the effectiveness of internal audit activity and enhance company profitability through efficient resource utilization. Risk-based auditing programs are designed to place audit resources in the areas of highest risk and enable an efficient and proactive risk assessment and control environment. This process necessitates and fosters cooperation and improved relationships between auditors and management.

Numerous large financial institutions have implemented trust department risk-based auditing programs as part of a corporate-wide, risk-based auditing system. Institution or holding company audit personnel that report to a trust department audit committee of the board typically administer these audit programs. This committee may report to another board audit committee or directly to the board.

Risk-based auditing programs are designed to be dynamic processes that focus on the identification and measurement of risk and the implementation of appropriate risk management systems. It requires, at a minimum, periodic risk assessments of all significant trust and asset management activities. These assessments are documented, reviewed and updated before a new audit of a specific activity has begun. While these audit programs and risk assessment models are primarily internally designed, there are a few vendors who are providing prototype shells, which the financial institution purchases and modifies to meet its particular needs.

The basic design standards of the risk-based auditing programs are similar. There are, however, significant variances in the risk assessment models and monitoring formats. The sophistication of each program will vary with the size, complexity, geographic diversity and technological capital of each financial institution. In designing the program and its components the auditors may work closely with trust department management in order to identify the various trust and asset management products and services and the risks associated with them.

The following is a brief summary of some steps that can be used to begin building an effective risk-based audit program.

- Develop an auditable universe and define auditable entities.

  The first step in the risk assessment process is to develop an auditable universe. Auditors should determine the significant trust and asset management activities of the organization and construct these activities into definable auditable entities. Auditable entities are most often established by business line but are also created by service or function.

- Develop an auditable entity business profile.

  A profile of each trust and asset management auditable entity is then developed that documents the entity's business goals and objectives, strategies, organizational structure and operating systems. The purpose of the profile is to identify key risks inherent in the entity and document the structure of risk management and internal control systems. Workflow analysis is sometimes performed at this stage, but is more frequently documented during the planning of actual audit work programs.

- Prepare the auditable entity risk assessment.

  The trust and asset management risk assessment format is typically structured to evaluate and measure business, inherent risk and control system risk. Within each of these categories, specific trust and asset management risk factors are listed for analysis and provided with a rating (usually numerical). The factors are supported by written standards with definitions and application guidelines. Risk factors vary in focus and number but examples of common factors include the following:

  - financial indicators such as account size and types, transaction volumes, growth trends and earnings;
  - control environment that includes the corporate risk culture, management style and organizational structure;
  - risk management and internal control systems;
  - management information systems and technology;
  - strategic factors such as product development and marketing focus; and
  - compliance, litigation and regulatory environment.

Some trust and asset management risk based audit programs have structured their risk assessment models to specifically address the nine risk categories that have been identified and promulgated by OTS.

Trust and asset management risk based systems may attempt to quantify the various risks through the application of a qualitative model rating system. The risk factors are often rated or scored based on a formalized scale such as High, Medium, or Low, or 1 through 5. Some systems may even apply a weighting factor to the process, which may be based upon the auditor's knowledge of the savings association's history versus industry averages or standards.

Programs may include the use of risk matrixes and charts that compare the risk and control aspects and then attempt to identify control or efficiency gaps. This type of analysis illustrates where business risk is equal to or different from the appropriate risk control level. This "gap" analysis concept is informally applied in the auditor's evaluation of risk and control systems. The matrixes and charts rarely stand on their own. Usually there is a narrative commentary accompanying the matrixes, which analyze and support the auditor's conclusions.

- Develop the trust and asset management risk-based auditing plan.

  Once the risk assessment process is completed, the auditor is now ready to develop his audit plan. The assessment process is used as the primary tool in developing the plan. The audit plan is a comprehensive document that is approved each year by the trust department audit committee or board. It establishes audit schedules, work program scope and resource allocations for each auditable entity.

- Audit execution, exception reporting and follow-up processes.

  Implementation of the trust department audit plan involves three key processes, planning, execution and reporting. During the planning stage, the auditable entity's risk profile is analyzed and a risk-based audit work program is developed which will be used to execute the audit of the specific activities. The auditing process will identify any exceptions found. In the reporting process, the auditor must determine what exception items are reportable in a formalized report and which are communicated to department management in an informal manner.

  Similar to the Uniform Trust Interagency Rating System used by OTS and the other banking regulators, each audit report may contain a rating, categorizing the auditor's overall findings regarding the auditable activity. An activity's overall rating will usually depend upon the amount and severity of exceptions found. The distribution of formalized audit reports may be impacted by the audit report rating with more critical reports receiving broader and higher level distribution.

  Once the report is distributed, the auditor must set up a system to monitor any actions taken by department management to resolve the auditor's concerns. The exception rating system may also impact the timing of the auditor's follow-up of audit exceptions. The follow-up program should require some form of monitoring for all exceptions regardless of their significance.

- Implement systems to monitor and update risk assessments.

  Prior to the next audit, the risk assessments will need to be reviewed and updated to reflect any changes from the last audit.

  Formally or informally, trust department auditors are provided periodic monitoring information reports for risk assessment purposes. The auditors use the information to adjust auditing priorities but an update of the risk assessment profile or matrix of the trust department may or may not be completed until the required annual assessment date or until an audit is conducted.

- Audits of One or More Affiliates

  With the continual growth in multi-bank and unitary thrift holding companies, many financial organizations now have one or more of its subsidiaries performing trust and asset management activities. Many of these holding companies will use their holding company internal auditors to perform audits of their subsidiaries' trust and asset management activities. In order to create efficiencies, many of these auditors will perform an audit of a specific function or functions for each of the trust and asset management subsidiaries at the same time rather than auditing a subsidiary institution's entire trust and asset management activities at one time. Upon the conclusion of their audit, the auditors will present the results of their audit (usually in one report) to the subsidiaries' audit committee(s).

  OTS does not object to this auditing method as long as the sample includes the functions performed by the savings association entity. However, the trust department audit committee should receive a presentation of findings in accordance with the requirements set forth in §550.480 and ensure monitoring practices are established to correct noted deficiencies.