pennsylvania
DEPARTMENT OF BANKING
AND SECURITIES

MARKET SQUARE PLAZA | 17 N SECOND STREET, SUITE 1300 | HARRISBURG, PA 17101-2290
Ph 717.787 2665 Fx 717 787 8773 W www banking state pa us

INTERNAL AUDIT PROGRAMS FOR FINANCIAL INSTITUTIONS
SECTION 1407 OF THE BANKING CODE OF 1965

Section 1407 of the Banking Code requires that all state-chartered institutions have an annual audit by a certified public accountant, including accounts held in a fiduciary capacity. For non-public institutions not covered by Section 36 of the Federal Deposit Insurance Act or Section 704.15(a) of the National Credit Union Administration Rules and Regulations, in lieu of the annual audit by a certified public accountant, an institution may adopt a system of continuous audits approved by the Pennsylvania Department of Banking and Securities as noted in Section 1407(c) of the Banking Code of 1965.

The board of directors and senior management are responsible for ensuring that an effective system of internal controls and an effective internal audit function is in place that is appropriate to the institution's size, nature, and scope of activities. The board of directors and senior management are also responsible for ensuring the importance of internal control is understood and respected throughout the institution. The overall responsibility cannot be delegated, although the design, implementation and monitoring of specific internal controls may be delegated. Outsourcing of the internal control program does not relieve the board of directors and senior management of their responsibility.

For those institutions that choose to satisfy Section 1407(c) of the Banking Code through an approved internal audit program, the following listed conditions must be satisfied·

Prior to Receiving Department Approval

The Board of Directors must adopt a resolution to submit a proposed continuous internal audit program to the Department for approval.

The Board of Directors must create the position of Auditor if it does not already exist.

If necessary, the Board must amend the bylaws to provide for the position of Auditor and the responsibilities of the position (The duties and the responsibilities of the Auditor must be free of operational duties and the Auditor must not be required to report to operating officers)

The Board of Directors must establish a responsibility line from the Board or its Audit Committee directly to the Auditor and require that the Auditor report only to this committee.

Submit Proposed Audit Program to the Department

The following items must be included with the submission:

1. A certified copy of the Board of Directors' resolution as indicated above, and if necessary, a copy of the amendment to the bylaws indicated above.

2. An analysis that considers the extent of auditing program that will effectively monitor the internal controls system. The analysis must include the costs and benefits of the internal audit function as compared to the costs and benefits of an external auditor.

3 A copy of the organizational chart showing reporting/responsibility lines of the Audit Department, including reporting of the Auditor to the Board of Directors or its Audit Committee. No operational duties or responsibilities should be assigned to the audit staff

4. Resumes of the Auditor and each member of the Audit Department staff (excluding nonprofessional staff) reflecting the educational and experience qualifications of each member. A minimum of one auditor must have professional certification in auditing or experience with the Institute of Internal Auditors' (IIA) "Standards for the Professional Practice of Internal Auditing".

In some cases, a prescheduled personal visitation by the responsible member of the Department's staff will meet with the Auditor and other applicable bank officials.

The Department will issue an approval letter when the proposed audit program meets the Department's audit coverage requirements. Approved audits will be subject to termination if the condition of the institution deteriorates to less than satisfactory.

Following Department Approval

The Auditor and/or Audit Committee must submit to the Board of Directors an annual summary report of the audits conducted during the year as required by Section 1407(c) of the Banking Code.

The summary report must state the degree of compliance with the approved audit program. Institutions are encouraged to evaluate their internal control against the Committee of Sponsoring Organizations of the Treadway Commission report *Internal Control-Integrated Framework.*

The summary report must include the Auditor's opinion on the adequacy of those internal control functions, as listed under "Minimum Requirements for an Approved Program," that are appropriate to the subject institution.

The Board of Directors must file a copy of the summary report with the Department within 30 days of submission to the Board of Directors.

All proposed revisions in the approved audit program and personnel must be submitted to the Department for approval prior to adoption.

At a minimum, the continuous audit program must be re-approved every three years by the board and must include an updated cost/benefit analysis comparison to an external audit.

Department bank examiners, at each examination, will review the program and the records maintained thereon to ascertain the adequacy and degree of adherence to the approved program All approved revisions will also be reviewed by the bank examiners.

Examiners will access the quality and scope of an institution's internal audit function and will consider:

Institution size
Nature, scope, and complexity of its activities
Risk profile
Actions taken or planned to minimize or eliminate identified weaknesses
The extent of the internal auditing program
Compensating controls
Adjustments for significant changes in the institution's environment, structure, activities, risk exposures, or systems

Other Requirements

The Auditor must have substantial independence in the areas being audited. More specifically, the Auditor must functionally report directly to the Board of Directors or the Audit Committee of the Board of Directors.

The minutes of the Board should be available to the Auditor so that the Auditor is aware at all times of the intention of management and can gear the program to the actions required.

The audit program should include procedures to give reasonable assurance to management and the Department that there are controls in place to assure compliance with the laws and regulations and management objectives. Internal audit activities must be conducted in accordance with professional standards, such as the Institute of Internal Auditor's *Standards for the Professional Practice of Internal Auditing*. These standards address independence, professional proficiency, scope of work, performance of audit work, management of internal audit, and quality assurance reviews

A control risk assessment (or risk assessment methodology) must be conducted on an annual basis.

An internal audit plan must be developed based on the control risk assessment and include the timing and frequency of planned internal audit work.

A detailed audit manual must be developed and include: (1) a description of the function or area to be audited, (2) a description of the internal controls applicable to the targeted function or area, and (3) procedures to be followed to accomplish the audit.

Audit reports must be provided for each audit that presents the purpose, scope, and results of the audit, including findings, conclusions (rating), and recommendations. Workpapers that document the work performed and support the audit report must be maintained.

Outsourcing Arrangements

If an outsourced vendor performs virtually all the procedures or tests of the system of internal controls, a designated manager of internal audit must oversee the vendor. The manager of internal audit is responsible for approving the scope, plan, and procedures to be performed.

Before entering into any outsourcing arrangement, the institution must perform due diligence to ensure the vendor has sufficient and qualified staff to perform the contracted work.

Minimum Audit Coverage by an Approved Internal Audit Program

The functions or areas to be covered by the audit program must include, at a minimum, the general areas listed below.

Real Estate Lending
Asset Management
Emerging Market and Trading Activities
Insider Transactions
Bank Secrecy Act
Bank Bribery Statue
Information Technology (Refer to Information Technology Audit Requirements below)
Compliance Management System

Information Technology (IT) Audit Requirements

IT audits assess the controls, accuracy, and integrity of the institution's information systems processing and technology infrastructure IT audits must cover the processing of transactions by servicing organizations, usually accomplished through an audit report produced in compliance with SASE 16. IT audits should cover, as applicable, the areas noted below.

User and data center support and delivery
Local and wide area networks
Telecommunications
Information security
Electronic data interchange
Development and acquisition
Business continuity and contingency planning
Data integrity
Confidentiality and safeguarding of customer information
IT risk management

Fiduciary Audit Requirements

At least once during each calendar year, the institution must have an audit of all significant fiduciary activities under the direction of its fiduciary audit committee. The board of directors' minutes must note the audit results, including significant actions taken in response to any audit finding. Institutions may adopt a continuous audit system under which the institution arranges for discrete audits of each significant fiduciary activity. Audit intervals should be commensurate with the nature and risk of fiduciary activities.

A fiduciary audit must ascertain whether the institution's internal control policies and procedures provide reasonable assurance that the institution is administering fiduciary activities in accordance with applicable law, properly safeguarding fiduciary assets, and accurately recording transactions in appropriate accounts in a timely manner. The fiduciary audit should also include the review of the institution's risk management and compliance function activities to assess their effectiveness in managing fiduciary activity risk. Activities that may require separate audit attention and reports include the activities noted below.

- Annual study and evaluation of internal accounting control reports of nonexempt registered transfer agents required by 17 CFR 240.17Ad-13
- Annual audits of collective investment funds in accordance with 12 CFR 9 18(b)(6).
- Annual financial statements based on audits of proprietary mutual funds in compliance with applicable securities laws.
- Internal control audits covering performance of certain fiduciary services for other organizations.
- External control audits, using criteria in SASE 16, covering functions that rely on the services of an outside organization.