

TO ALL BANKS, BANK AND TRUST COMPANIES, SAVINGS BANKS AND TRUST COMPANIES:

This guidance is issued to clarify the acceptable means for compliance with the audit requirements of Section 1407 of the Banking Code of 1965 (the “Banking Code”), in light of the amendments to audit thresholds found in 12 CFR Part 363 issued by the Federal Deposit Insurance Corporation in November 2025. This guidance rescinds and replaces any previous guidance issued by the Commonwealth of Pennsylvania, Department of Banking and Securities (the “Department”) regarding Section 1407 of the Banking Code. In accordance with Section 1407 of the Banking Code, an institution must either have (1) an annual audit made by certified public accountants (“CPA”) and a report signed by the CPA, or (2) a system of internal audit control approved by the Department and an annual report made by the Auditor/Comptroller. *See Addendum A.*

Annual Audit and Audit Report by Certified Public Accountant

In accordance with Section 1407(a) and (b) of the Banking Code, all banks, bank and trust companies, savings banks and trust companies are required to (1) conduct an annual audit of the books and affairs of the institution completed by a CPA “Financial Audit” and (2) submit a report of the Financial Audit signed by the CPA (“Financial Audit Report”). The Financial Audit must include any accounts held in a fiduciary capacity. Consistent with Section 1407(d), audits submitted to the institution’s primary federal regulator pursuant to federal statutes and regulations satisfy the Section 1407(a) requirement. Further, institutions may continue to submit an audit that is compliant with federal law to satisfy Section 1407, even if not required by the applicable federal regulator. For example, audits compliant with 12 CFR §363.2 would satisfy the Section 1407(a) requirement.

System of Internal Audit Control Approved by the Department and Summary Report

An institution which has a system of internal audit control approved by the Department pursuant to Section 1407(c) of the Banking Code, may, in *lieu* of a CPA performing the Financial Audit, choose instead to submit to the Board of Directors or Trustees (the “Board”) and file with the Department an annual summary report (“Summary Audit Report”) prepared by the institution’s Auditor/Comptroller. The Summary Audit Report must:

1. Be based on a system of internal audit control approved by the Department (“Approved Audit Program”).
2. Address the same matters as the Financial Audit required by Section 1407(a).
3. Set forth the degree of compliance with the Approved Audit Program.
4. Express an opinion of the Auditor/Comptroller as to the adequacy of the internal controls.

For those institutions that choose to satisfy the Section 1407(a) Financial Audit requirement through an Approved Audit Program under Section 1407(c), the requirements hereinafter must be satisfied. Approved Audit Programs may be subject to termination by the Department if the Approved Audit Program is no longer appropriate based on the overall condition of the institution or if an onsite examination determines that the audit program no longer meets the standards of this guidance.

The Department reserves the right to conduct prescheduled visitations to meet with the Auditor/Comptroller and other applicable bank officials to discuss and review the proposed audit program prior to a final decision being made regarding the adequacy of the program.

Requirements for a System of Internal Audit Control

To ensure that the institution's audit program is an effective risk management tool capable of providing reasonable assurance to the Board, senior management, and other stakeholders, the following components are required when submitting a Section 1407(c) audit program request to the Department on the form and in the manner as set forth in Addendum B.

Organizational Structure

- The Board must adopt a resolution stating their intent to submit a Section 1407(c) request to the Department seeking an Approved Audit Program.
- The Board must create the position of Auditor/Comptroller, if it does not already exist, supported by a written job description.
- If necessary, the Board must amend their bylaws to provide for the position of Auditor/Comptroller and the responsibilities of the position.
- The audit department and audit staff must be independent and free from any conflicts of interest, with a direct reporting line to the audit committee or Board outlined in the financial institution's organizational chart. No operational duties or responsibilities may be assigned to the audit staff.
- A minimum of one audit department staff member must have professional certification in auditing or experience with the Institute of Internal Auditors' ("IIA") Global Internal Audit Standards.

Administration and Documentation

- An internal audit policy that outlines the scope, objectives, and responsibilities of the audit program and audit department staff, as well as record retention requirements. This policy is to be reapproved annually by the Board.
- Audit program procedures that provide for the minutes of the Board to be made available to the Auditor/Comptroller as soon as they are available. This will allow the Auditor/Comptroller to be aware, at all times, of the intentions and strategies of the Board and management so that changing risks can be considered and the audit program adjusted accordingly.
- An ethics policy or code of ethics that promotes the professionalism and principles that the audit department staff must uphold. A means for reporting a breach of this policy or code to the audit committee must also be included. This policy or code of ethics is to be reapproved annually by the Board.
- A comprehensive risk assessment to aid in audit planning. This risk assessment is to be conducted at least on an annual basis and presented to the audit committee for ratification.
- An internal audit plan developed based on the results of the risk assessment, which includes the timing and frequency of planned internal audit work. This internal audit plan must be reviewed on an annual basis in conjunction with the risk assessment and presented to the audit committee for ratification.



- A detailed manual for each audit area that describes the objective of the audit, the applicable internal controls, and procedures to be performed to test the effectiveness of the internal controls of that audited area. Periodic reviews should be performed regarding the content and quality of the manuals.
- Audit reports for each audited area that present 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 for a period of at least seven years.
- A mechanism for tracking audit and examination findings and progress made towards remediation. This tracking document should be presented to the audit committee on a periodic basis.

Minimum Audit Program Coverage

The audit program must be designed in a manner that allows for an opinion to be formed regarding the institution's conformity to and adequacy of internal controls over financial reporting ("ICFR"). This will be completed through the audit procedures designed by the Auditor/Comptroller, which may include the completion of workpapers, review of various forms of documentation, sampling of transactions, data integrity checks, confirmations, and discussions with the auditee. The scope and depth of the audit program will ultimately be determined by the Auditor/Comptroller and Board, or audit committee based on the results of the institution's risk assessment.

As a basis for reviewing the adequacy of the Section 1407(c) request, the Department expects the areas below and any related balance sheet and income statement accounts to be included, as these typically have the greatest impact on the accuracy or production of the financial statements or may pose a higher risk for fraud. The Auditor/Comptroller may choose to include other areas that are identified through completion of the risk assessment, such as new areas that may materially impact the financial statements or are at a high risk for fraudulent activity. Regardless of the operational function, any relevant accounting estimates, off-balance sheet items, and transactions highly susceptible to manipulation should be included in the review and completion of the audit.

- | | |
|--|--|
| ❖ Loans and Leases | ❖ Investment and Derivatives |
| ❖ Allowance for Credit Losses | ❖ Crypto-related Activities |
| ❖ Deposits | ❖ Capital Accounts |
| ❖ Wire Transfers | ❖ Payroll |
| ❖ Cash & Due from Banks | ❖ Entity Level Operations and Governance |
| ❖ Borrowed Funds | ❖ Regulatory Reporting |
| ❖ Accounts Payable and Expenses | ❖ New Products |
| ❖ Other Assets/Liabilities | ❖ Merger and Acquisition Transactions |
| ❖ Taxes and DTAs/DTLs | ❖ Interest Accruals |
| ❖ Insider and Related Party Transactions | ❖ Information Systems |
| ❖ Mortgage Banking | ❖ Fiduciary Activities (as applicable) |

Information Systems

Information systems are utilized in various capacities at financial institutions, including the processing of daily transactions and for compiling financial data. As such, including information systems in the scope of the audit program is a critical part of the institution's ICFR process. Accordingly, the audit program must include relevant testing of internal controls over information

systems utilized at the institution in relation to financial reporting. The testing of controls should be commensurate with the institution's information technology risk profile, determined through the information technology risk assessment process.

Fiduciary Activities (as applicable)

The institution must audit all significant fiduciary activities and accounts held in a fiduciary capacity. Institutions may adopt an ongoing 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 activities 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 activities 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 the 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 SSAE 18 covering functions that rely on the services of an outside organization

Authoritative Resources

- The audit program and associated internal controls should provide reasonable assurance of compliance with applicable laws and regulations and management objectives. Internal audit activities must be conducted in accordance with professional standards, such as the IIA's Global Internal Audit Standards.
- Institutions are encouraged to evaluate their internal control framework against the Committee of Sponsoring Organizations of the Treadway Commission report Internal Control-Integrated Framework (ICIF-2013).
- The Banking Code of 1965, as amended, 7 P.S. § 101 *et seq.*

Annual Summary Report

The Auditor/Comptroller must submit to the Board a Summary Audit Report of the audits conducted during the year as required by Section 1407(c) of the Banking Code. The audits and associated report must conform to the accounting standards and principles pursuant to 12 U.S.C. § 1831n, as noted in Section 1407(d) of the Banking Code. This includes compliance with Generally Accepted Accounting Principles of the United States.

Within 30 days of submission to the Board, the institution must file a copy of the summary report with the Department. The summary report must include the following information, at a minimum:

- Audit reporting period
- Audits conducted with their current and prior risk ratings
- Exceptions identified along with the status of remediation for those exceptions
- If any exceptions identified materially impact the financial statements, an explanation of what steps will be taken to correct and reissue the financial statements
- The associated effects any new product or service offerings have on the risk profile of the institution and the audit program
- The current direction of overall risk compared to prior year
- A summary of any reports of unethical or fraudulent activity identified and steps taken to investigate these reports
- A summary of any ongoing or future litigation that will materially impact the financial statements
- The institution's level of compliance with applicable state and federal regulatory requirements and the impact of any non-compliance on the financial statements
- The Auditor/Comptroller's opinion on the adequacy of the internal control functions in place and degree of institutional compliance with the approved audit program
- The impact any changes in accounting rules and guidance had on the current year financial statements

Audit Program Revisions and Reapprovals

The risk assessment used to form the basis of the institution's Section 1407(c) audit program should be reviewed annually by the Auditor/Comptroller and Board to ensure that the program remains appropriate for the institution's risk profile. All proposed revisions to the Approved Audit Program must be submitted to the Department for approval prior to adoption. Additionally, the institution must inform the Department of any changes to the professional staff in the audit department. Resumes of newly hired staff must be included in communication to the Department.

The institution's election to utilize an Approved Audit Program must be re-approved by the Board at least once every three years, reflected via written resolution, and must include an updated cost-benefit analysis. This resolution will be reviewed during the next onsite examination. If the program is terminated, the Department must be notified immediately.

Outsourcing Arrangements

If an outsourced, non-CPA 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 with ratification by the audit committee. The vendor must have direct communication access to the Board and audit committee. The vendor must be given access to applicable records and staff for the effective completion of the audit procedures. Additionally, a summary report of the audit(s) completed, and exceptions identified, must be reported to the Board or audit committee in a timely manner. Workpapers are to be reviewed by audit department personnel and retained for a

minimum of seven years. An opinion on the adequacy of the internal control functions in place and degree of institutional compliance with the Approved Audit Program is still required.

Before entering into any outsourcing arrangement, the institution must perform thorough vendor due diligence. Ongoing due diligence is to continue throughout the contracted period.

ADDENDUM A

Section 1407 of the Banking Code provides as follows:

- (a) Annual audit** – Except as provided in subsection (c) of this section, the board of directors or trustees shall at least once each year have made, by certified public accountants selected by the institution and satisfactory to the department, an audit of the books and affairs of the institution including such matters as may be required by the department and including, in the case of a bank and trust company, a savings bank or a trust company, accounts held in a fiduciary or other representative capacity. The department may by regulation establish minimum standards for audits and reports under this subsection (a).
- (b) Audit report** – A report of the audit made under subsection (a) of this section shall be signed by the certified public accountants who make it and filed with the department and a signed copy of the report shall be submitted to the board and kept in the files of the institution.
- (c) Internal auditors** – In the case of an institution which has a system of internal audit control approved by the department, no audit under subsection (a) of this section shall be required and in lieu of the report required by subsection (b), the auditor or comptroller of the institution shall submit to the board an annual summary report of the same matters as those required under subsection (a) of this section. Such report shall set forth the degree of compliance with the approved audit system and shall express the opinion of the auditor or comptroller as to the adequacy of the internal controls. The report shall be kept in the files of the institution and a copy shall be filed with the department.
- (d) Accounting standards** – Audits and reports shall be deemed to satisfy the requirements of this section to the extent the audits and reports conform to accounting standards and principles applicable pursuant to 12 U.S.C. §1831n to reports or statements required to be filed with the Federal banking agencies.



ADDENDUM B

SECTION 1407(c) AUDIT PROGRAM REQUEST FORM

Instructions: This form is to be completed and provided along with the required documentation as follows: for banks, bank and trust companies or savings banks to ra-bndepannualaudit@pa.gov; for non-depository trust companies to ra-bntrustaudit@pa.gov. Failure to provide the required documentation may delay or cease the Department of Banking and Securities' ability to review and provide a decision on the financial institution's request. The Chairperson of the Audit Committee must sign this form attesting that the Section 1407(c) internal audit program request is authorized by the institution and that the required documentation has been included. By signing, the Chairperson also agrees on behalf of the institution, to further communication from the Department regarding this request. This communication may include requests for additional information, documentation, or interviews with institution personnel via email correspondence, telephone calls, up to a pre-scheduled onsite visitation by Department personnel.

FINANCIAL INSTITUTION NAME: _____

DATE OF SUBMISSION: _____

FINANCIAL INSTITUTION CONTACT INFORMATION FOR QUESTIONS RELATING TO THIS SUBMISSION:

NAME: _____

PHONE NUMBER: _____

EMAIL ADDRESS: _____

CHAIRPERSON SIGNATURE: _____

SUBMISSION CHECKLIST:

- ☐ A certified copy of the Board of Directors' or Trustees' resolution, and if applicable, a copy of the amendment to the bylaws.
- ☐ The job description of the Auditor/Comptroller.
- ☐ The analysis that considered the costs and benefits of the audit program as compared to the costs and benefits of engaging an external CPA firm, with a narrative summary explaining why bank officials chose the alternative annual audit procedures allowed by Section 1407(c) in lieu of an external CPA firm.
- ☐ A copy of the organizational chart showing the reporting line of the audit department.
- ☐ Resumes of the Auditor/Comptroller and each member of the audit department staff (excluding nonprofessional staff) reflecting the education and professional experience of each member.
- ☐ The internal audit policy outlining the scope, objectives, and responsibilities of the audit program and audit department staff. Board minutes are to be included evidencing approval of the policy.
- ☐ The ethics policy or code of ethics promoting the professionalism and principles that audit department staff must uphold. A means for reporting a breach of this policy or code to the audit committee must also be included. Board minutes are to be included evidencing approval of the policy.
- ☐ The annual comprehensive risk assessment developed to aid in audit planning. Audit committee minutes are to be included evidencing ratification of the risk assessment by the audit committee.
- ☐ The current year audit plan developed based on the risk assessment that includes the timing and frequency of planned internal audit work. Audit committee minutes are to be included evidencing ratification of the audit plan by the audit committee.
- ☐ An example of an audit manual developed by the Auditor/Comptroller. Additional manuals may be requested during the review process.
- ☐ An example of an audit report developed by the Auditor/Comptroller. Additional audit reports and workpapers may be requested during the review process.
- ☐ The mechanism developed for tracking audit and examination findings.