

TABLE OF CONTENTS

Number	Date	Subject
BL-92-81	12-24-81	Financial Information on Data Centers
BL-2-87	01-25-88	Risks Associated with End-User Computing Operations and Suggested Control Policies See FFIEC Policy SP-3 for details
BL-35-88	12-05-88	FFIEC Supervisory Policy on LSIS See FFIEC Policy SP-4 for details
BL-22-88	07-14-89	Contingency Planning for Financial Institutions See FFIEC Policy SP-5 for details
FIL-17-90	03-05-90	FFIEC Statement on EDP Service Contracts See FFIEC Policy SP-6 for details
FIL-30-93	04-29-93	Interagency Statement Addressing Risks from Switches and Network Services in Retail EFT Systems See FFIEC Policy SP-9 for details
FIL-13-94	02-25-94	FFIEC Statement on Electronic Imaging Systems See FFIEC Policy SP-10 for details

NEWS RELEASES

PR-104-78	10-18-78	Federal Regulatory Agencies Adopt Joint System for Rating Data Processing Centers See FFIEC Policy SP-2 for details
-----------	----------	---

POLICY STATEMENTS

Effective Date	Subject
12-28-88	Statement of Policy Regarding Independent External Auditing Programs of State Nonmember Banks
01-22-90	Statement of Policy Providing Guidance on External Auditing Procedures for State Nonmember Banks

Note: BANK LETTERS - BL and Financial Institution Letters - FIL

FEDERAL DEPOSIT INSURANCE CORPORATION

FINANCIAL INFORMATION ON DATA CENTERS

BL-92-81
December 24, 1981

To: CHIEF EXECUTIVE OFFICERS OF INSURED STATE NONMEMBER BANKS

Subject: Financial Information on Data Centers

Financial institutions have become increasingly dependent on the computer to process daily transactions. This processing is often contracted to independent data processing companies (servicers) without properly evaluating the operations of the servicer. The FDIC is concerned that many serviced institutions fail to obtain sufficient financial data to analyze the servicer's financial condition. Since data processing services are essential to the daily operation of those serviced institutions, the FDIC has adopted the following policy statement:

Financial institutions that contract for data processing services with independent servicers should obtain and analyze annual financial statements (preferably audited and unconsolidated) to assure themselves of the servicer's continued financial viability. The right to obtain this information should be included in the service contract. If the servicer's financial condition is unsound or shows signs of serious deterioration, this problem should be closely monitored while alternative contingency plans are pursued.

/s/ Quinton Thompson
Director

FEDERAL DEPOSIT INSURANCE CORPORATION

END-USER COMPUTING

BL-2-87

January 25, 1988

To: CHIEF EXECUTIVE OFFICERS OF INSURED STATE NONMEMBER BANKS

Subject: Risks Associated with End-User Computing Operations and Suggested Control Policies

Attached is a joint issuance by the Federal Financial Institutions Examination Council on risks associated with end-user computing activities. End-user computing is recognized as a necessary and important aspect of information processing and delivery for many financial institutions. The issuance discusses some of the potential risks and possible controls for these activities. An appropriate level of supervision and control, consistent with guidelines offered in this circular, is expected for each insured state nonmember bank and savings bank utilizing end-user computing systems.

The purpose of this Bank Letter is to alert management at each financial institution to the risks associated with end-user computing operations and to encourage the implementation of sound control policies over such activities.

In recent years, microcomputers, or "personal computers" (PCs), have become more prominent in the business environment. They are now being used not only as word processors and access devices to other computers, but also as powerful stand-alone computers. As such, information processing has evolved well beyond the traditional central environment to distributed or decentralized operations. This trend has offered substantial benefits in productivity, customization, and information access. However, it also has meant that those control procedures, previously limited to the central operations, must be reapplied and extended to the "end-user" level.

Technology, using microcomputers as end-user computing devices, has taken data processing out of the centralized, control environment and introduced computer-related risks in new areas of financial institutions. However, the implementation of these new information delivery and processing networks has out paced the implementation of controls. Basic controls and supervision of these computer activities often have not been introduced, or expected, at the end-user level. The technological advantages, expediency, and cost benefits of end-user computing have been the primary focus. Recognition of the increased exposures and the demands for expanded information processing controls has lagged. These concerns for data protection and controlled operations within the end-user environments must be addressed to minimize risks from:

- incorrect management decisions,
- improper disclosure of information,
- fraud,
- financial loss,
- competitive disadvantage, and
- legal or regulatory problems.

End-user computing is recognized as a productive and appropriate operational activity. However, control policies for data security and computer operations, consistent with those for centralized information processing functions, need to address the additional risks represented in the end-user computing operations.

Management in each financial institution is encouraged to evaluate the associated risks with its end-user computing networks and other forms of distributed computer operations. Control practices and responsibilities to manage these activities should be incorporated into an overall corporate information security policy. This policy should address areas such as:

- management controls,
- data security,
- documentation,
- data/file storage and back-up,
- systems and data integrity,
- contingency plans,
- audit responsibility, and
- training.

Responsibilities for the acquisition, implementation and support of such networks should be clearly established.

The appendix to this Bank Letter provides more details regarding the risks and suggested controls for end-user computing and other computer-related activities. Additional control recommendations are contained in the FFIEC EDP Examination Handbook.

It is the responsibility of the Board of Directors to ensure that appropriate corporate policies, which identify management responsibilities and control practices for all areas of information processing activities, have been established. The existence of such a "corporate information security policy," the adequacy of its standards, and the management supervision of such activities will be evaluated by examiners during the regular supervisory reviews of the institution.

/s/ Paul G. Fritts
Director

See FFIEC Policies SP-3 for details.

FEDERAL DEPOSIT INSURANCE CORPORATION

LARGE-SCALE INTEGRATED FINANCIAL SOFTWARE SYSTEMS (LSIS)

BL-35-88
December 5, 1988

To: CHIEF EXECUTIVE OFFICERS OF INSURED STATE NONMEMBER BANKS

Subject: FFIEC Supervisory Policy on LSIS

Attached is an issuance of the Federal Financial Institutions Examination Council on risks associated with large-scale integrated financial software systems (LSIS). The issuance alerts financial institutions to the potential risks of these systems and the possible controls appropriate for their development, implementation and use.

Large-scale integrated systems are software products that combine several banking applications in one package. Such software is becoming more common, particularly among larger banks, as a means of improving the institutions' information systems. Bank executives and directors should be aware of, and concerned about, the potential problems with these systems. Supervision and controls, consistent with the guidelines contained in this issuance, are expected at each bank using LSIS.

/s/ Paul G. Fritts
Director

See FFIEC Policies SP-4 for details.

FEDERAL DEPOSIT INSURANCE CORPORATION

CONTINGENCY PLANNING FOR FINANCIAL INSTITUTIONS

BL-22-88
July 14, 1989

To: CHIEF EXECUTIVE OFFICERS OF FDIC-SUPERVISED BANKS

Subject: FFIEC Supervisory Policy on Contingency Planning

Attached is an issuance of the Federal Financial Institutions Examination Council on the need for contingency planning at financial institutions. The issuance also addresses issues that should be considered when developing a viable contingency plan.

Contingency planning is a process of establishing strategies to minimize disruption of services and financial loss, and ensure timely resumption of operations in the event of a disaster. Such planning requires an institution-wide emphasis and is equally important for financial institution servicers as well as financial institutions.

It is the responsibility of the Board of Directors to ensure that a comprehensive contingency plan has been implemented. The contingency plan will be evaluated by examiners during the regular supervisory reviews of the institution.

/s/ Paul G. Fritts
Director

See FFIEC Policies SP-5 for details.

FEDERAL DEPOSIT INSURANCE CORPORATION

EDP SERVICE CONTRACTS

FIL-17-90
March 5, 1990

To: CHIEF EXECUTIVE OFFICER

Subject: FFIEC Statement on EDP Service Contracts

Attached is an issuance of the Federal Financial Institutions Examination Council on the potential risks in contracting for EDP services and/or failing to properly account for certain contract provisions.

It is the responsibility of each institution to ensure that all contracts for vital services are properly reflected on the institution's books and on Call Reports submitted to regulatory authorities. Examiners will evaluate service contracts during the regulatory supervisory review of your institution.

/s/ Paul G. Fritts
Director

See FFIEC Policies SP-6 for details.

FEDERAL DEPOSIT INSURANCE CORPORATION

ELECTRONIC FUNDS TRANSFER (EFT) SYSTEMS

FIL-30-93
April 29, 1993

TO: CHIEF EXECUTIVE OFFICER

**SUBJECT: Interagency Statement Addressing Risks from Switches and Network
Services in Retail EFT Systems**

Attached is a statement of the interagency Federal Financial Institutions Examination Council (FFIEC) on the risks associated with switch and network services in retail electronic funds transfer (EFT) systems. An EFT network is the combination of interconnected terminals and computers that process fund transfers and other electronic messages among participating financial institutions. The switch is the computer system that facilitates the transfer of these electronic messages between the terminals and the appropriate participants. The FFIEC statement does not address wholesale or large dollar transfer systems such as FEDWIRE and CHIPS.

Recognizing the growing importance of electronic banking, the FFIEC statement makes clear that financial institutions are responsible for ensuring that there are sufficient controls covering switch processing, that contracts adequately define participants' liabilities and responsibilities, and that settlement procedures do not pose undue risk to an institution. The statement outlines the responsibilities of an institution's board of directors and senior management, and it lists the controls that should be in place in an EFT switch or network environment. Examiners will evaluate EFT switches and network services during the regular supervisory review of each institution.

For further information about the issues addressed in the attached statement, please contact your regional office of the FDIC's Division of Supervision.

/s/ Paul G. Fritts

Executive Director

See FFIEC Policies SP-9 for details.

FEDERAL DEPOSIT INSURANCE CORPORATION

ELECTRONIC IMAGING SYSTEMS

FIL-13-94
February 25, 1994

To: CHIEF EXECUTIVE OFFICER

Subject: Interagency Statement On Risks from Electronic Imaging Systems

Attached is a statement of the interagency Federal Financial Institutions Examination Council (FFIEC) on the risks associated with electronic imaging systems. Imaging systems are used to capture, index, store, and retrieve electronic images of paper documents. The FFIEC paper discusses some potential risks to consider when planning for and using imaging technology.

The FFIEC statement outlines security and control issues which institutions should address when considering imaging systems. Examiners will evaluate electronic imaging systems during the regular supervisory review of each institution.

For further information about the issues addressed in the attached statement, please contact your regional office of the FDIC's Division of Supervision.

/s/ Stanley J. Poling
Director

See FFIEC Policies SP-10 for details.

FEDERAL DEPOSIT INSURANCE CORPORATION

FEDERAL REGULATORY AGENCIES ADOPT JOINT SYSTEM FOR RATING DATA PROCESSING CENTERS

**PR-104-78
10-18-78**

The Federal bank and thrift institution regulators today announced a joint system for rating data processing centers.

The system is to become effective immediately. It was adopted by the Office of the Comptroller of the Currency (supervisor of national banks), the Federal Reserve Board (supervisor of State chartered member banks), the Federal Deposit Insurance Corporation (supervisor of State chartered non-member banks and of insured mutual savings banks) and by the Federal Home Loan Bank Board (supervisor of federally chartered savings and loan associations).

Under the new rating system the four agencies will apply uniform standards to data centers that are operated by banks or thrift institutions supervised by one of the four agencies and to other data processing centers serving such banks or thrift institutions.

The uniform data processing center rating system follows adoption by the Federal regulators earlier this year of a joint policy for the examination of data processing centers operated by or serving financial institutions they supervise.

Under the joint rating system:

- A performance rating system is established based on the evaluation of four critical functions: audit, management, systems development and programming, and computer operations.
- Ratings of these functions are combined into a composite rating.

The attached copy of the rating system gives a general description of the individual composite and performance ratings.

Distribution: Insured State Nonmember Banks (Commercial and Mutual)

See FFIEC Policies SP-2 for details.

STATEMENT OF POLICY REGARDING INDEPENDENT EXTERNAL AUDITING PROGRAMS OF STATE NONMEMBER BANKS

12-28-88

1. In view of its interest in the financial soundness of banks and the banking system, the FDIC believes that a strong internal auditing function combined with a well-planned *external auditing program*¹ substantially lessens the risk that a bank will not detect potentially serious problems. An external auditing program is a set of procedures designed to test and evaluate high *risk areas* a bank's business which are performed by an *independent* auditor who may or may not be a *public accountant*. The failure to detect and correct potentially serious problems increases the risk a bank poses to the FDIC's insurance fund. A strong internal auditing function establishes the proper control environment and promotes accuracy and efficiency in a bank's operations. An external auditing program complements this function by providing an objective outside view of the bank's operations.
2. Regardless of the strength of a bank's internal auditing procedures, the FDIC believes that an external auditing program should be considered by a bank's board of directors as part of the cost of operating a bank in a safe and sound manner. An external auditing program assists the bank's board of directors in safeguarding assets and identifying risks inherent in its operation. In addition, an external auditing program may tend to assist directors in the event of litigation on whether an institution's board has exercised reasonable care in protecting the assets of the bank. Thus, the FDIC urges all state nonmember banks to establish and maintain a sound external auditing program.
3. The FDIC strongly encourages the board of directors of each state nonmember bank to establish an *audit committee*, consisting, if possible, *entirely of outside directors*. The audit committee or board of directors of each state nonmember bank generally should analyze the extent of the external auditing coverage needed by the bank annually. They should determine whether the bank's needs will best be met by an *audit* of its *financial statements* or by an acceptable alternative (described in paragraphs 8 and 9 below). When selecting the scope of the planned external auditing program for the year, the committee or board should ensure that the program will provide sufficient substantive external coverage of the bank's risk areas and any other areas of potential concern, such as compliance with applicable laws and regulations.

If not, additional external auditing procedures conducted by an independent auditor may be appropriate for a specific year or several years to cover particularly high risk areas of the bank. The decisions resulting from these deliberations should be recorded in the committee's or board's minutes.

4. If the audit committee or board of directors of a bank, after due consideration, determines not to engage an independent public accountant to conduct an annual audit of the bank's financial statements (or whose parent holding company's consolidated financial statements are not audited), the reasons for the committee's or board's conclusion to use one of the acceptable alternatives or to have no external auditing program should be documented in its minutes. In the evaluation, the committee or board generally should consider not only the cost of an annual audit of the bank's financial statements, but also the potential benefits.

¹ Terms defined in Appendix A are italicized the first time they appear in this statement of policy.

5. A review of both a bank's internal and external auditing programs has been and will continue to be a part of the FDIC's examination procedures. FDIC examiners will review the nature of each bank's external auditing program in conjunction with the risk areas perceived in that particular bank's business and operations, and they will exercise their judgment and discretion in evaluating the adequacy of a bank's external auditing program. Examiners will not automatically comment negatively to the board of directors of a bank with an otherwise satisfactory external auditing program merely because it does not engage an independent public accountant to perform an audit of its financial statements.

Audit by an Independent Public Accountant

6. The FDIC strongly encourages each state nonmember bank to adopt an external auditing program that includes an annual audit of its financial statements by an independent public accountant. A bank that does so would generally be considered to have a satisfactory external auditing program. An external audit of a bank's financial statements benefits management by assisting in the establishment of the accounting and operating policies, internal controls, internal auditing programs, and management information systems necessary to ensure the fair presentation of these statements. An audit also assists boards of directors in fulfilling their fiduciary responsibilities and provides them greater assurance that financial reports are accurate and provide adequate disclosure.
7. An audit of a bank's financial statements performed by the independent public accountant as of a quarter-end date when the Reports of Condition and Income are prepared is preferable and would permit the bank to use the audited financial statements in the preparation and/or subsequent review of those reports. A bank may also find it more cost effective to be audited during accounting firms' less busy periods. The independent public accountant chosen should be experienced in auditing banks and knowledgeable about banking regulations in order to provide the bank with the most effective service.

Alternatives to an Audit by a Public Accountant

8. The FDIC recognizes that a bank's audit committee or board of directors may determine that the external auditing program that will best meet its individual needs for that particular year will be other than an audit of its financial statements by an independent public accountant. The committee or board, after a full review of alternative and/or supplemental approaches for an adequate independent external auditing program, may decide on a well-planned *directors' examination*, independent analysis of internal controls or other areas, a *report on the balance sheet*, specified auditing procedures by an independent auditor. If the bank has an outside auditing firm that is simply obtaining confirmations of deposits and loans, for example, the committee or board should normally expand the scope of the auditing work performed to include additional procedures to test the bank's high risk areas.
9. Nonaccounting firms with bank auditing experience and expertise that are independent of the bank are available in some geographic locations. They may provide acceptable directors' examinations, analyses, or specified auditing work at a reasonable cost. In some instances, these firms' services include nonauditing work which enables them to provide suggestions on compliance issues and operational efficiencies. Depending upon the expertise of the firm and the scope of the engagement, these nonaccounting firms may be an appropriate choice for an external auditing program.

Newly Insured Banks

10. The FDIC believes that an adequate external auditing program performed by an independent auditor should be an integral part of the safe and sound management of a bank. Thus, applicants for deposit insurance coverage after the effective date of this statement of policy will generally be expected to commit their bank to obtain an audit of their financial statements by an independent public accountant annually for at least the first three years after deposit insurance coverage is granted.² The FDIC may determine on a case-by-case basis that an independent audit of financial statements is unnecessary where an applicant can demonstrate that the benefits derived from such an external audit will be substantially provided by other outside sources, or where the applicant is owned by another company and will undergo an audit performed by an independent public accounting firm as part of an audit of the consolidated financial statements of its parent company.

Notification and Submission of Reports

11. Whether currently or newly insured, the FDIC requests each state nonmember bank that undergoes any external auditing work, regardless of the scope of the work, to furnish a copy of any reports by the public accountant or other external auditor, including any management letters, to the appropriate FDIC regional office as soon as possible after their receipt by the bank.
12. In addition, the FDIC requests each bank to promptly notify the appropriate FDIC regional office when any public accountant or other external auditor is initially engaged to perform external auditing procedures and when a change in its accountant or auditor occurs.

Holding Company Subsidiaries

13. When the audit committee or board of directors of any state nonmember bank owned by another company (such as a bank holding company) considers its external auditing program, it may find it appropriate to express the scope of its program in terms of the bank's relationship to the consolidated group. No section of this statement of policy is intended to imply that any state nonmember bank owned by another company is expected to obtain a separate audit of the financial statements of the individual bank. Where the state nonmember bank is directly or indirectly included in the audit of the consolidated financial statements of its parent company performed by an independent public accounting firm, the state nonmember bank may send one copy of the comparable reports by the public accountant or notification of the change in accountants for the consolidated company to the appropriate regional director. If several banks copy of the comparable reports by the public accountant or notification of the change in accountants for the consolidated company to the appropriate regional director. If several banks supervised by the same FDIC regional office are owned by one parent company, a single copy of each report applicable to the consolidated company may be submitted to the regional office on behalf of all of the affiliated banks.

² Operating non-FDIC insured institutions should also note that the FDIC expects, unless waived in writing by the FDIC, any applicant for insurance with more than \$50 million in assets to have an audit of its financial statements prior to submitting an application, and requests that a copy of the auditor's report be included as part of the application. The FDIC may require such an audit, on a case-by-case basis, for applicants with assets of \$50 million or less. Refer to the June 9, 1987 Statement of Policy Regarding Applications for Federal Deposit Insurance by Operating Non-FDIC Insured Institutions, as amended June 24, 1987.

Troubled Banks

14. An annual independent external auditing program complements both the FDIC's supervisory process and bank internal auditing programs by further identifying or clarifying issues of potential concern or exposure. It can also greatly aid management in taking corrective action, particularly when weaknesses are detected in internal control or management information systems. For these reasons, an annual audit of bank financial statements performed by an independent public accounting firm or, if more appropriate, specified auditing procedures will be a condition of future enforcement actions, when deemed necessary, or if it appears that any of the following conditions may exist:
 - (a) Internal controls and internal auditing procedures are inadequate;
 - (b) The directorate is generally ununiformed in the area of internal controls;
 - (c) There is evidence of insider abuse;
 - (d) There are known or suspected defalcations;
 - (e) There is known or suspected criminal activity;
 - (f) It is probable that director liability for losses exists;
 - (g) Direct verification is warranted; and/or
 - (h) Questionable transactions with affiliates have occurred.

15. Such an enforcement action may also require that (a) the bank provide to the appropriate FDIC regional office a copy of the auditor's report and any management letter received from the auditor promptly after the completion of any auditing work and that (b) the bank notify the regional office in advance of the time and date of any meeting between management and the auditor at which any auditing findings are to be presented so that a representative of the FDIC may be present if the FDIC so chooses.

Appendix A -- Definitions

Audit. An examination of the financial statements, accounting records, and other supporting evidence of a bank performed by an independent certified or licensed public accountant in accordance with generally accepted auditing standards and of sufficient scope to enable the auditor to express an opinion on the bank's financial statements as to their presentation in accordance with generally accepted accounting principles (GAAP).

Audit Committee. A committee of the board of directors, consisting, if possible, entirely of outside directors. To the extent possible, members of the committee should be knowledgeable about accounting and auditing. They should be responsible for reviewing and approving the bank's internal and external auditing programs or recommending adoption of these programs to the full board. Both the internal auditor and the external auditor should have unrestricted access to the audit committee without the need for any prior management knowledge or approval. Other duties of the audit committee should include reviewing the independence of the external auditor annually, being consulted by management when it seeks a second opinion on an accounting issue, overseeing the quarterly regulatory reporting process, and reporting its findings periodically to the full board.

Directors' Examination. A review by an independent third party that has been authorized by the bank's board of directors and is performed in accordance with the board's analysis of potential risk areas. Certain procedures may also be required as a result of state law. A directors' examination consisting solely of such procedures as cash counts and confirmations of loans and deposits would not normally be considered a well-planned director's examination. (Sometimes directors' examinations are similar to so-called "engagement audits" or "operational audits." Nevertheless, no widely accepted national standards exist for the specific procedures that must be performed in directors' examinations or these "audits.")

External Auditing Program. The performance of procedures to test and evaluate high risk areas of a bank's business by an independent auditor, who may or may not be a public accountant, sufficient for the auditor to be able to express an opinion on the financial statements or to report on the results of the procedures performed.

Financial Statements. The statements of financial position, income, cash flows (changes in financial position), and changes in shareholders equity together with related notes.

Independent. certified public accountant, public accountant, or other auditor will be recognized as independent who is not in fact independent. (Reference is made to Section 335.604 of the FDIC rules and regulations for the complete definition of the term "independent.")

Outside Directors. Members of a bank's board of directors who are not officers, employees, or principal stockholders of the bank, its subsidiaries, or its affiliates, and do not have any material business dealings with the bank, its subsidiaries, or its affiliates.

Public Accountant. A certified public accountant or licensed public accountant who is duly registered and in good standing as such under the laws of the place of his/her residence or principal office, who is licensed by the accounting regulatory authority of his/her state, and who possesses a permit to practice public accountancy.

Report on the Balance Sheet. An examination of the balance sheet, accounting records, and other supporting evidence performed by an independent certified or licensed public accountant in accordance with generally accepted auditing standards.

Risk Areas. The risk areas are those particular activities of a specific bank that expose the bank to potential losses if problems were to exist and go undetected. The highest risk areas in banks generally include, but are not necessarily limited to, the valuation of collectibility of loans (including the Reasonableness of the allowance for loan losses, investments, and repossessed and foreclosed collateral; internal controls; and insider transactions.

By order of the Board of Directors, November 16, 1988.

**STATEMENT OF POLICY PROVIDING GUIDANCE
ON EXTERNAL AUDITING PROCEDURES
FOR STATE NONMEMBER BANKS**

01-22-90

In its Statement of Policy Regarding Independent External Auditing Programs of State Non-member Banks that became effective December 28, 1988, the FDIC strongly encourages each state nonmember bank to have an annual audit¹ of its financial statements performed in accordance with generally accepted auditing standards by an independent public accountant. Nevertheless, the board of directors of each state nonmember bank is ultimately responsible for safeguarding the bank's assets and ensuring the integrity of its financial statements. The audit committee or board of directors of the bank may determine not to engage an independent public accountant to perform an audit for various reasons. In those instances, the FDIC recommends that each state nonmember bank have an independent external auditor² (who need not be an independent public accountant) annually perform the auditing procedures³ set forth below as part of its external auditing program.

Although the purpose of this policy statement is to encourage certain basic external auditing procedures as a less costly alternative for banks choosing not to have a financial statement audit, the auditing procedures recommended in this guidance are basic to any sound external auditing program. For that reason, they should also be among the procedures performed by an independent public accountant in an audit in which an opinion is expressed on a bank's financial statements. Thus, if a bank chooses to have an audit of its financial statements performed by an independent public account, such an opinion audit will generally satisfy the objectives of this statement of policy.

The auditing procedures contained in this statement of policy are intended to address high risk areas common to all banks. However, they do not address all possible risks in a banking organization and each bank must review the risks inherent in its particular business to determine if additional procedures are needed to cover other high areas in which it has activities. For example, if a bank or its subsidiaries has significant real estate investments, securities broker-dealer or similar activities (including those described in Section 337.4 of the FDIC risk rules and regulations), or trust department operations, among others, the FDIC urges the bank to consider expanding the scope of its external auditing program so that it includes auditing procedures in these other high risk areas. (Information on external auditing procedures applicable to other banking activities is available from banking industry trade associations and auditing organizations.)

¹ Reference is made to appendix A to the Statement of Policy Regarding Independent External Auditing Programs of State Nonmember Banks for the definitions of terms used in this statement of policy.

² Ibid.

³ When a bank engages an independent public accountant to perform less than a full financial statement audit, the engagement letter describing the procedures for which the bank has contracted generally refers to the work as "agreed-upon procedures." The term "auditing procedures" used throughout this statement of policy is meant to encompass these "agreed-upon procedures."

The independent auditor (or the public accountant) should be informed of and permitted access to all examination reports, administrative orders, and any additional written communication between the bank and the FDIC or state banking authorities.⁴ The auditor should obtain bank management's written representation that he has been informed of and granted access to all such documents prior to the completion of his field work.

A review of both a bank's internal and external auditing programs will continue to be part of the FDIC's examination procedures, but examiners will not automatically comment negatively upon a bank that does not have an audit or all of these auditing procedures performed annually by an independent auditor. The examiner will review the risks in each bank's business and operations, and will comment negatively if internal auditing is deficient and/or sufficient external auditing procedures are not performed as often as necessary to assure the safe and sound operation of the bank under examination.

Extent of Testing

Where the procedures set forth below require testing or determinations to be made, sampling may be used. Both judgmental and statistical sampling may be acceptable methods of selecting samples to test. Judgmental sampling may be particularly suitable for small banks, and sample sizes should be selected consistent with generally accepted auditing standards (for the certified public accountant) or as agreed upon by the auditor and bank client. In any event, the sampling method and extent of testing (including the minimum sample size(s) used) should be disclosed in the auditor's report.

As with any auditing program under generally accepted auditing standards or otherwise, if an auditing procedure that is set forth below deals with an area or account of the bank in which the amounts and/or risks are not material to the bank's operations and financial results based on the experience and judgment of the auditor, the procedure may be omitted from that year's auditing program. Nevertheless, the auditor would have to review each such area or account each year in order to determine whether to reaffirm his/her conclusion.

Reports to be Filed with the FDIC

The FDIC's Statement of Policy Regarding Independent External Auditing Programs of State Nonmember Banks requests that each bank that undergoes any external auditing work, regardless of the scope of the work, furnish a copy of the reports pertaining to the external auditing program, including any management letters, to the appropriate FDIC regional office as soon as possible after their receipt by the bank. In addition, that policy statement requests each bank to promptly notify the appropriate FDIC regional office when any independent public accountant or other external auditor is initially engaged to perform external auditing procedures and when a change in its accountant or auditor occurs.

External Auditing Procedures Required by State Banking Regulators

Some state statutes or state banking authorities require certain auditing procedures (often called

⁴ In this regard, section 931 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 provides that "Each insured depository institution which has engaged the services of an independent auditor to audit such depository institution within the past 2 years shall transmit to such auditor*** a copy of the most recent report of examination received by such depository institution." In addition, each depository institution is required by section 931 to provide such auditor with a copy of any supervisory memorandum of understanding with the depository institution, any written agreement between any federal or state banking agency and the institution, and any report of any action initiated or taken by a federal banking agency under section 8 of the Federal Deposit

Insurance Act (or similar state action) or any civil money penalty assessed against the depository institution or any institution-affiliated party.

"Directors' Examinations") to be performed each year with a report submitted to the state authority. Assuming the state requirements on scope and reporting correspond to or exceed those recommended in this statement of policy and the auditing procedures are performed by an independent external auditor, the bank may satisfy this statement of policy when its state-mandated external auditing program is performed. A copy of the auditor's report prepared for the state may be submitted in lieu of a separate report to the FDIC.

Holding Company Subsidiaries

When the audit committee or board of directors of any state nonmember bank owned by another company (such as a bank holding company) considers its external auditing program, it may find it appropriate to express the scope of its program in terms of the bank's relationship to the consolidated group. If the state nonmember bank is directly or indirectly included in the audit of the consolidated financial statements of its parent company performed by an independent public accounting firm, this statement of policy is not intended to imply that the bank is expected to have separate external auditing procedures performed. Nevertheless, if the board of directors of the subsidiary bank determines that the bank has activities that involve unusual risks to the subsidiary and these activities were not addressed by the audit of the consolidated entity (because these risks may be immaterial to the consolidated entity), appropriate additional external auditing procedures may need to be considered for the subsidiary bank.

As provided in the FDIC's Statement of Policy Regarding Independent External Auditing Programs of State Nonmember Banks, where a bank is directly or indirectly included in the audit of a consolidated entity's financial statements, the bank may send one copy of the comparable reports by the public accountant or the notification of a change in accountants for the consolidated company to the appropriate regional director. If several banks supervised by the same FDIC regional office are owned by one parent company, a single copy of each report applicable to the consolidated company may be submitted to the regional office on behalf of all of the affiliated banks.

Basic External Auditing Procedures

Loans

1. Inquire as to whether the bank has policies that address the lending and collection functions. Review the bank's loan policies to ascertain whether they address the following items:
 - a. General fields of lending in which the bank will engage and the types of loans within each field;
 - b. Descriptions of the bank's normal trade area and circumstances under which the bank may extend credit to borrowers outside of such area;
 - c. Limitations on the maximum volume of each type of loan product in relation to total assets;
 - d. Responsibility of the board of directors in reviewing, ratifying or approving loans;
 - e. Leading authority of the loan or executive committee (if such a committee exists) and individual loan officers or classes of officers;
 - f. Adherence to legal lending limits;
 - g. Types of loans, specifying whether secured and unsecured, which will be granted;
 - h. Circumstances under which extensions or renewals of loans are permitted;
 - i. Guidelines for rates of interest and terms of repayment for loans;
 - j. Documentation required by the bank for each type of loan;
 - k. Limitations on the amount advanced in relation to the value of various types of collateral;

-
- l. Limitations on the extension of credit through overdrafts;
 - m. Level or amount of loans granted in specific industries or specific geographic locations;
 - n. Guidelines for participations purchased and/or sold;
 - o. Guidelines for documentation of new loans prior to approval, updating loan files throughout the life of the loan, and maintenance of complete and current credit files on each borrower;
 - p. Guidelines for loan review procedures by bank personnel including:
 - i. An identification or grouping of loans that warrant the special attention of management;
 - ii. For each loan identified, a statement or indication of the reason(s) why the particular loan merits special attention; and
 - iii. A mechanism for reporting periodically to the board on the status of each loan identified and the action(s) taken by management.
 - q. Collection procedures, including, but not limited to, actions to be taken against borrowers who fail to make timely payments;
 - r. Guidelines for nonaccrual loans (i.e., when an asset should be placed in nonaccrual status, individuals responsible for identifying nonperforming assets and placing them in nonaccrual status, and circumstances under which an asset will be placed back on accrual);
 - s. Guidelines for loan charge-offs;
 - t. Guidelines for in-substance foreclosures.
2. Read the board of directors' minutes to determine that the loan policies have been reviewed and approved. Through review of the board of directors' minutes and through inquiry of executive officers, determine whether the board of directors revises the policies and procedures periodically as needed.
 3. Obtain the minutes of the board of directors and/or loan committee, as appropriate, and, through a comparison of a sample of loans made throughout the period with lending policies, test whether loans funded during the previous year were properly authorized by the appropriate committee or loan officer(s) and within the bank's lending limits.
 4. Select a sample of borrowers (including loans from each major secured and unsecured loan company) and determine through examination of loan files and other bank reports whether lending and collection policies are being followed (e.g., type of loan and any extension or renewal of a previous loan are in accordance with loan policy, funds were not advanced until after loan approval was received from proper loan authorization level, and insurance coverage is adequate with the bank named as loss payee).
 5. Using the sample of borrowers selected from each major category of secured loans, determine through examination of files and other bank reports whether collateral policies are being followed (e.g., loan is adequately collateralized, documentation is present and properly prepared, and assignments are perfected).
 6. If material, review policies for lending on floor plan merchandise, warehouse inventory, and accounts receivable to determine that limitations on such loans and directions on verification of collateral by bank inspection are included in the policies. Ascertain that implementing procedures have been established and test for compliance by responsible bank personnel.

-
7. Determine whether participations purchased and participations sold transactions have been reported to and authorized by the board of directors or loan committee, if applicable, through review of appropriate minutes.
 8. Confirm a sample of participations purchased and participations sold with participating banks to verify that they are legitimate transactions and that they are properly reflected as being with or without recourse in the bank's records.
 9. Balance detail ledgers or reconcile computer-generated trial balances with the general ledger control accounts for each major category of loans, including loans carried as past due or in a nonaccrual status.
 10. Confirm a sample of all loans within each major category, including past due and nonaccrual loans.
 11. From reports to the board on the status of loans identified as warranting special attention, review the disposition of a sample of loans no longer appearing on these reports.
 12. Test loan interest income and accrued interest by:
 - a. determining the bank's method of calculating and recording interest accruals;
 - b. obtaining trial balances of accrued interest;
 - c. testing the reconciliation of the trial balances to the general ledger;
 - d. determining that interest accruals are not made on nonaccrual loans;
 - e. select sample items from each major category of loans and:
 - i. determining the stated interest rate and appropriate treatment of origination fees and costs,
 - ii. testing receipt of payments and correctness of entries to applicable general ledger accounts,
 - iii. calculating accrued interest and comparing it to the trial balance, and
 - iv. reviewing recorded book value for appropriate accretion of discount (net origination fees) and amortization of premium (net origination costs); and
 - f. performing an analytical review of yields on each major category of loan for reasonableness.

Allowance for Loan Losses

1. Test charge-offs and recoveries for proper authorization and/or reporting by reference to the board of directors' minutes. Review charged-off loans for any relationship with bank insiders or their related interests.
2. Review the bank's computation of the amount needed in the allowance for loan losses as of the end of the most recent quarter. Documentation should include consideration of the following matters:
 - a. General, local, national and international (if applicable) economic conditions;
 - b. Trends in loan growth and depth of lending staff with expertise in these areas;
 - c. Concentrations of loans (e.g., by type, borrower, geographic area, and sector of the economy);
 - d. The extent of renewals and extensions to keep loans current;
 - e. The collectibility of nonaccrual loans;

-
- f. Trends in the level of delinquent and classified loans compared with previous loan loss and recovery experience;
 - g. Results of regulatory examinations; and
 - h. The collectibility of specific loans on the "watch list" taking into account borrower financial status, collateral type and value, payment history, and potential permanent impairment.

Securities

1. Review the investment policies and procedures established by the bank's board of directors (BOD). Review the BOD (or investment committee) minutes for evidence that these policies and procedures are periodically reviewed and approved. The policies and procedures should include, but not be limited to:
 - a. Investment objectives, including use of "held for sale" and trading activities;
 - b. Permissible types of investments;
 - c. Diversification guidelines to prevent undue concentration;
 - d. Maturity schedules;
 - e. Limitation on quality ratings;
 - f. Hedging activities and other uses of futures, forwards, options, and other financial instruments;
 - g. Handling exceptions to standard policies;
 - h. Valuation procedures and frequency;
 - i. Limitations on the investment authority of officers; and
 - j. Frequency of periodic reports to the BOD on securities holdings.
2. Test the investment procedures and ascertain whether information reported to the BOD (or investment committee) for securities transactions is in agreement with the supporting data by comparing the following information on such reports to the trade tickets for a sample of items (including futures, forwards, and options):
 - a. Descriptions
 - b. Interest rate
 - c. Maturity
 - d. Par value, or number of shares
 - e. Cost
 - f. Market value on date of transaction (if different than cost).
3. Using the same sample items, analyze the securities register for accuracy and confirm the existence of the sample items by examining securities physically held in the bank and confirming the safekeeping of those securities held by others.
4. Balance investment subledger(s) or reconcile computer-generated trial balances with the general ledger control accounts for each type of security.
5. Review policies and procedures for controls which are designed to ensure that unauthorized transactions do not occur. Ascertain through reading of policies, procedures, and BOD minutes whether investment officers and/or appropriate committee members have been properly authorized to purchase/sell investments and whether there are any limitations or restrictions on delegated responsibilities.
6. Obtain a schedule of the book, par, and market values of securities as well as their rating classifications. Test the accuracy of the market values of a sample of securities and compare

the ratings listed to see that they correspond with those of the rating agencies. Review the bank's documentation on any permanent declines in value that have occurred among the sample of securities to determine that any recorded declines in market value are appropriately computed. Examine the bank's computation of the allowance account for securities, if any, for proper presentation and adequacy.

7. Test securities income and accrued interest by:
 - a. determining the bank's method of calculating and recording interest accruals;
 - b. obtaining trial balances of accrued interest;
 - c. testing the reconciliation of the trial balances to the general ledger;
 - d. determining that interest accruals are not made on defaulted issues;
 - e. selecting items from each type of investment and money market holdings and:
 - i. determining the stated interest rate and most recent interest payment date of coupon instruments by reference to sources of such information that are independent of the bank,
 - ii. testing timely receipt of interest payments and correctness of entries to applicable general ledger accounts,
 - iii. calculating accrued interest and comparing it to the trial balance,
 - iv. reviewing recorded book value for appropriate accretion of discount and amortization of premium;
 - f. performing an analytical review of yields on each type of investment and money market holdings for reasonableness.

8. Review investment accounts for volume of purchases, sales activity and length of time securities have been held. Inquire as to the bank's intent and ability to hold securities until maturity. (If there is frequent trading in an investment account, such activity may be inconsistent with the notion that the bank has the intent and ability to hold securities to maturity.) Test gains and losses on disposal of investment securities by sampling sales transactions and:
 - a. determining sales prices by examining invoices or brokers' advices;
 - b. checking for the use of trade date accounting and the computation of book value on trade date;
 - c. determining that the general ledger has been properly relieved of the investment, accrued interest, premium, discount and other related accounts;
 - d. recomputing the gain or loss and compare to the amount recorded in the general ledger; and
 - e. determining that the sales were approved by the BOD or a designated committee or were in accordance with policies approved by the BOD.

Insider Transactions

1. Review the bank's policies and procedures to ensure that extensions of credit to and other transactions with insiders⁵ are addressed. Ascertain that these policies include specific guidelines defining fair and reasonable transactions between the bank and insiders and test insider transactions for compliance with these guidelines and statutory and regulatory requirements. Ascertain that the policies and procedures on extensions of credit comply with the requirements of Federal Reserve Regulation O.

-
2. Obtain a bank-prepared list of insiders, including any business relationships they may have other than as a nominal customer. Also obtain a list of extensions of credit to and other transactions that the bank, its affiliates, and its subsidiaries have had with insiders that are outstanding as of the audit date or that have occurred since the prior year's external auditing procedures were performed. Compare these lists to those prepared for the prior year's external auditing program to test for completeness.
 3. Review the board of directors' minutes, loan trial balances, supporting loan documentation, and other appropriate bank records in conjunction with the list of insiders obtained from the bank to verify that a sample of extensions of credit to and transactions with insiders were:
 - a. in compliance with bank policy for similar transactions and were at prevailing rates and terms at that time;
 - b. subjected to the bank's normal underwriting criteria and deemed by the bank to involve no more than a normal degree of risk or present no other unfavorable features;
 - c. approved by the board of directors in advance with the interested party abstaining from voting; and
 - d. within the aggregate lending limits imposed by Regulation O or other legal limits.
 4. Review the bank's policies and procedures to ensure that expense accounts of individuals who are executive officers, directors, and principal shareholders are addressed and test a sample of the actual expense account records for compliance with these policies and procedures.

Internal Controls

General Accounting and Administrative Controls

1. Review the board of directors' minutes to verify that account reconciliation policies have been established and approved and are reviewed periodically by the BOD. Determine that management has implemented appropriate procedures to ensure the timely completion of reconciliations of accounting records and the timely resolution of reconciling items.
2. Determine whether the bank's policies regarding segregation of duties and required vacations for employees (including those involved in the EDP function) have been approved by the BOD, and verify that these policies and the implementing procedures established by management are periodically reviewed, are adequate, and are followed.
3. Confirm a sample of deposits in each of the various types of deposit accounts maintained by the bank. Inquire about controls over dormant deposit accounts.
4. Test to determine that reconciliations are prepared for all significant asset and liability accounts and their related accrued interest accounts, if any, such as "due from" accounts; demand deposits; NOW accounts; money market deposit accounts; other savings deposits; certificates of deposits; and other time deposits. Review reconciliations for:
 - a. timeliness and frequency;
 - b. accuracy and completeness; and
 - c. review by appropriate personnel with no conflicting duties.
5. Compare a sample of balances per reconciliations to the general ledger and supporting trial balances.

-
6. Examine detail and aging of a sample of reconciling items from those accounts whose reconciliations have been tested and reviewed and a sample of items in suspense, clearing, and work-in-process accounts by:
 - a. testing aging;
 - b. determining whether items are followed up on and appropriately resolved on a timely basis; and
 - c. discussing items remaining on reconciliations and in the suspense account with appropriate personnel to ascertain whether any should be written off. Review a sample of charged-off reconciling and suspense items for proper authorization.

 7. Verify through inquiry and observation that the bank maintains adequate records of its off-balance sheet activities, including, but not limited to, its outstanding letters of credit and its loan commitments. Review the bank's procedures for monitoring the extent of its credit exposure from such activities to determine whether probable or reasonably possible losses exist.

Electronic Data Processing Controls

1. Read the BOD's minutes to determine whether the BOD has reviewed and approved the bank's electronic data processing (EDP) policies (including those regarding outside servicers, if any, and the in-house use of individual personal computers (PCs) and personalized programs for official bank records) at least annually, confirm that management has established appropriate implementing procedures, and verify the bank's compliance with these policies and procedures.
 - a. The policies and procedures for either in-house processing or use of an outside service center should include:
 - i. a contingency plan for continuation of operations and recovery when power outages, natural disasters, or other threats could cause disruption and/or major damage to the institution's data processing support (including compatibility of servicer's plan with that of the bank);⁶
 - ii. requirements for EDP-related insurance coverage which include the following provisions:
 - (1) extended blanket bond fidelity coverage to employees of the bank or servicer;
 - (2) insurance on documents in transit, including cash letters; and
 - (3) verification of the insurance coverage of the bank or service bureau and the courier service;
 - iii. review of exception reports and adjusting entries approved by supervisors and/or officers;
 - iv. controls for input preparation and control and output verification and distribution;
 - v. "back-up" of all systems, including off-premises rotation of files and programs;
 - vi. security to ensure integrity of data and system modifications; and
 - vii. necessary detail to ensure an audit trail.

⁶ For further guidance, see the July 1989, FFIEC Policy on Contingency Planning for Financial Institutions and Section 5 of the FFIEC EDP Examination Handbook.

-
- b. When an outside service center is employed, the policies and procedures should address the following additional items:
 - i. the requirement for a written contract for each automated application detailing ownership and confidentiality of files and programs, fee structure, termination agreement, and liability for documents in transit;
 - ii. review of each contract by legal counsel; and
 - iii. review of each third party review of the service bureau, if any.⁷
 2. In the area of general EDP controls, determine through inquiry and observation that policies and procedures have been established for:
 - a. Management and user involvement and approval of new or midfield application programs;
 - b. Authorization, approval and testing of system software modifications;
 - c. The controls surrounding computer operations processing;
 - d. Restricting access to computer operations facilities and resources including:
 - i. off-premises storage of master disks and PC disks;
 - ii. security of the data center and bank's PCs; and
 - iii. use and periodic changing of passwords.
 3. With respect to EDP applications controls, inquire about and observe:
 - a. The controls over:
 - i. Input submitted for processing,
 - ii. Processing transactions,
 - iii. Output,
 - iv. Applications on PCs, and
 - v. Telecommunications both between and within bank offices;
 - b. The security over unissued or blank supplies of potentially negotiable items; and
 - c. The control procedures on wire transfers including:
 - i. Authorizations and agreements with customers, including who may initiate transactions,
 - ii. Limits on transactions, and
 - iii. Call back procedures.

Auditor's Report to the Bank's Board of Directors

After the completion of the auditing procedures (or agreed-upon procedures) set forth above, the independent auditor should evaluate the results of his/her auditing work. The auditor should prepare and promptly submit a report addressed to the board of directors (or audit committee) of the bank detailing the findings and suggestions resulting from the performance of these auditing procedures.

Independent auditors should include in their report, as a minimum, (1) the accounts or items on which the procedures were applied; (2) the sampling method(s) used; (3) the procedures and agreed-upon extent of testing performed; (4) the accounting basis (either generally accepted accounting principles [GAAP] or the instructions for the preparation of the Reports of Condition and Income [Call Reports]) on which the accounts of items being audited are reported; (5) the auditor's findings; and (6) the date as of which the procedures were performed. The auditor should sign and date the report, which should also disclose the auditor's business address. The report submitted by an independent auditor who is a certified public

⁷ For further guidance on using a third-party report, see the American Institute of Certified Public Accountant's Audit and Accounting Guide, Audits of Service-Center Produced Records.

accountant should be rendered in accordance with the requirements of Statement on Auditing Standards (SAS) No. 35, "Special Reports-Applied Agreed-upon Procedures to Specified Elements, Accounts, or Items of a Financial Statement," and SAS No. 62, "Special Reports." Other independent auditors may wish to refer to these auditing standards for guidance in preparing their reports.

The bank is requested to send a copy of this report to the appropriate FDIC regional office as soon as possible after its receipt.

By order of the Board of Directors, January 16, 1990.