



Federal
Financial
Institutions
Examination
Council

Information Systems

VOLUME 2

REFERENCES

1996

FFIEC IS Examination Handbook

IS

FFIEC INFORMATION SYSTEMS EXAMINATION

HANDBOOK – 1996 EDITION

*This Information Systems Examination Handbook is an update of the January 1994 FFIEC IS Examination Handbook and replaces all previously published versions.
To obtain additional copies of the Handbook, contact the appropriate agency:*

FFIEC MEMBER AGENCIES:

Board of Governors of the Federal Reserve System

Publication Services
Washington, DC 20551
<http://www.bog.frb.fed.us>

Federal Deposit Insurance Corporation

DOS - Administrative Section
550 17th Street, N.W., Room 5009
Washington, DC 20429
<http://www.fdic.gov>

National Credit Union Administration

1775 Duke Street
Alexandria, VA 22314-3428
<http://www.ncua.gov>

Office of the Comptroller of the Currency

Communications Division
250 E Street, S.W.
Washington, DC 20219
<http://www.occ.treas.gov>

Office of Thrift Supervision

Communication Services Division
1700 G Street, N.W.
Washington, DC 20552
<http://www.ots.treas.gov>

PARTICIPATING FEDERAL AGENCY:

Farm Credit Administration

Office of Examination
1501 Farm Credit Drive
McLean, VA 22102-5090
<http://www.fca.gov>

**FFIEC
Information
Systems
Examination
Handbook**

Volume 2

Sponsored by the following FFIEC member agencies:

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision**

Participating Federal agency:

Farm Credit Administration

TABLE OF CONTENTS

VOLUME 2 - Section III LAWS AND POLICIES

Chapter 24	Laws and Regulations	24-1
	<i>(FFIEC Disk #2 and File Name S3C24.wpd)</i>	
	Introduction	24-1
	Bank Service Corporation Act - 12 USC 1861	24-1
	Bank Holding Companies - Regulation Y - 12CFR 225	24-4
	Financial Institutions Reform, Recovery, and Enforcement Act of 1989 - 12 USC 1811	24-4
	FDIC Improvement Act of 1991 - Part 363	24-5
	Table 24.1 IS Law and Regulation References	24-25
Chapter 25	Federal Financial Institution Examination Council (FFIEC) Policies	25-1
	<i>(FFIEC Disk #2 and File Name S3C25.wpd)</i>	
Chapter 26	Federal Deposit Insurance Corporation (FDIC) Policies	26-1
	<i>(FFIEC Disk #2 and File Name S3C26.wpd)</i>	
Chapter 27	Board of Governors of the Federal Reserve System (FRB) Policies	27-1
	<i>(FFIEC Disk #2 and File Name S3C27.wpd)</i>	
Chapter 28	National Credit Union Administration (NCUA) Policies	28-1
	<i>(FFIEC Disk #2 and File Name S3C28.wpd)</i>	
Chapter 29	Office of the Comptroller of the Currency (OCC) Policies	29-1
	<i>(FFIEC Disk #2 and File Name S3C29.wpd)</i>	
Chapter 30	Office of Thrift Supervision (OTS) Policies	30-1
	<i>(FFIEC Disk #2 and File Name S3C30.wpd)</i>	

VOLUME 2 - Section IV OTHER REFERENCES AND TOOLS

Glossary	31-1
<i>(FFIEC Disk #2 and File Name S4C31.wpd)</i>	

Summary of Contents:

Introduction 24- 1

Bank Service Corporation Act - 12 USC 1861 - 1867 24- 1

Bank Holding Companies - Regulation Y - CFR 225 24- 4

**Financial Institutions Reform, Recovery,
and Enforcement Act of 1989 - 12 USC 1811** 24- 5

FDIC Improvement Act of 1991 - Part 363 24- 5

Table 24-1 IS Laws and Regulations Reference 24-26

INTRODUCTION

This section contains statutory requirements applicable to information systems examinations.

Bank Service Corporation Act

*(Public Law 87-856, October 23, 1962 as amended)
Title 12, U.S. Code, Sec. 1861 et seq.
Chapter 18 – Bank Service Corporations*

Sec. 1861(1)¹ Short Title and Definitions

- (a) This chapter may be cited as the "Bank Service Corporation Act".
- (b) For the purpose of this Act-
 - (1) the term "appropriate Federal Banking agency" shall have the meaning provided in section 1813(q) of this title;
 - (2) the term "bank service corporation" means a corporation organized to perform service authorized by this chapter, all of the capital

stock of which is owned by one or more insured banks;

- (3) the term "Board" means the Board of Governors of the Federal Reserve System;
- (4) the term "depository institution" means an insured bank, a financial institution subject to examination by the Federal Home Loan Bank Board or the National Credit Union Administration Board, or a financial institution the accounts or deposits of which are insured or guaranteed under State law and are eligible to be insured by the Federal Deposit Insurance Corporation, the Federal Savings and Loan Insurance Corporation, or the National Credit Union Administration Board;
- (5) the term "insured bank" shall have the meaning provided in section 1813(h) of this title;
- (6) the term "invest" includes any advance of funds to a bank service corporation, whether by the purchase of stock, the making of a loan, or otherwise, except a payment for rent earned, goods sold and delivered, or services rendered prior to the making of such payment; and

¹ Numbers in parentheses in this section refer to section numbers in the Bank Service Corporation Act.

-
- (7) the term "principal investor" means the insured bank that has the largest dollar amount invested in the capital stock of a bank service corporation. In any case where two or more insured banks have equal dollar amounts invested in a bank service corporation, the corporation shall prior to commencing operations, select one of the insured banks as its principal investor and shall notify the bank's appropriate Federal banking agency of that choice within 5 business days of its selection.

Sec. 1862(2) Amount of Investment in Bank Service Corporation

Notwithstanding any limitation or prohibition otherwise imposed by any provision of law exclusively relating to banks, an insured bank may invest not more than 10 per centum of paid-in and unimpaired capital and unimpaired surplus in a bank service corporation. No insured bank shall invest more than 5 per centum of its total assets in bank service corporations.

Sec. 1863(3) Permissible Bank Service Corporation Activities for Depository Institutions (Perry Institutions)

Without regard to the provisions of sections 1864 and 1865 of this title, an insured bank may invest in a bank service corporation that performs, and a bank service corporation may perform, the following services only for depository institutions: check and deposit sorting and posting, computation and posting of interest and other credit and charges, preparation and mailing of checks, statements, notices, and similar items or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depositor institution.

Sec. 1864(4) Permissible Bank Service Corporation Activities for Other Persons

- (a) *Services permissible other than taking deposits*
A bank service corporation may provide to any person any service authorized by this section, except that a bank service corporation shall not take deposits.
- (b) *Services to be performed in State where shareholders are located*

Except with the prior approval of the Board under

section 1865(b) of this title in accordance with subsection (f) of this section –

- (1) a bank service corporation shall not perform the services authorized by this section in any State other than that State in which its shareholders are located; and
- (2) all insured bank shareholders of a bank service corporation shall be located in the same State.
- (c) *Performance where State bank is shareholder*

A bank service corporation in which a State bank is a shareholder shall perform only those services that such State bank shareholder is authorized to perform under the law of the State in which such State bank operates and shall perform such services only at locations in the State in which such State bank shareholder could be authorized to perform such services.

- (d) *Performance where national bank is shareholder*

A bank service corporation in which a national bank is a shareholder shall perform only those services that such national bank shareholder is authorized to perform under the law of the United States and shall perform such services only at location in the State at which such national bank shareholder could be authorized to perform such services.

- (e) *Performance where State bank and national bank are shareholders*

A bank service corporation that has both national bank and State bank shareholders shall perform only those services that may lawfully be performed by both its national bank shareholder or shareholders under the law of the United States and its State bank shareholder or shareholders under the law of the State in which such State bank or banks operate and shall perform such services only at location in the State at which both its State bank and national bank shareholders could be authorized to perform such services.

- (f) *Geographic location*

Notwithstanding the other provisions of this section or any other provision of law, other than the provisions of Federal and State branching law

regulating the geographic location of banks to the extent that those laws are applicable to an activity authorized by this subsection, a bank service corporation may perform at any geographic location any service, other than deposit taking, that the Board has determined, by regulation, to be permissible for a bank holding company under section 1843(c)(8) of this title.

Sec. 1865(5) Prior Approval for Investments in Bank Service Corporations

(a) Approval of Federal banking agency

No insured bank shall invest in the capital stock of a bank service corporation that performs any service under authority of subsection (c), (d), or (e) of section 1864 of this title without the prior approval of the bank's appropriate Federal banking agency.

(b) Approval of Board

No insured bank shall invest in the capital stock of a bank service corporation that performs any service under authority of section 1864(f) of this title and no bank service corporation shall perform any activity under section 1864(f) of this title without the prior approval of the Board.

(c) Considerations in determining approval

In determining whether to approve or deny any application for prior approval under this section, the Board or the appropriate Federal banking agency, as the case may be, is authorized to consider the financial and managerial resources and future prospects of the bank or banks and bank service corporation involved, including the financial capability of the bank to make a proposed investment under this chapter, and possible adverse effects such as undue concentration of resources, unfair or decreased competition, conflicts, of interest, or unsafe or unsound banking practices.

(d) Failure to act on application for approval

In the event the Board or the appropriate Federal banking agency, as the case may be, fails to act on any application under this section within ninety days of the submission of a complete application to the agency, the application shall be deemed approved.

Sec. 1866(6) Services to Nonstockholders

No bank service corporation shall unreasonably discriminate in the provision of any services authorized under this chapter to any depository institution that does not own stock in the service corporation on the basis of fact that the nonstockholding institution is in competition with an institution that owns stock in the bank service corporation, except that-

- (1) it shall not be considered unreasonable discrimination for a bank service corporation to provide services to a nonstockholding institution only at a price that fully reflects all of the costs of offering those services, including the cost of capital and a reasonable return thereon; and
- (2) a bank service corporation may refuse to provide services to a nonstockholding institution if comparable services are available from another source at competitive overall costs, or if the providing or services would be beyond the practical capacity of the service corporation.

Sec. 1867(7) Regulation and Examination of Bank Service Corporations

(a) Principal investor

A bank service corporation shall be subject to examination and regulation by the appropriate Federal banking agency of its principal investor to the same extent as its principal investor. The appropriate Federal banking agency of the principal shareholder of such a bank service corporation may authorize any other Federal banking agency that supervises any other shareholder of the bank service corporation to make such an examination

(b) Applicability of section 1818 of this title

A bank service corporation shall be subject to the provisions of section 1818 of this title as if the bank service corporation were an insured bank. For this purpose, the appropriate Federal banking agency shall be the appropriate Federal banking agency of the principal investor of the bank service corporation.

(c) Services performed by contract or otherwise

Notwithstanding subsection (a) of this section, whenever a bank that is regularly examined by an appropriate Federal banking agency, or any subsidiary or affiliate of such a bank that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises-

- (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the bank itself on its own premises, and
- (2) the bank shall notify such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first.

(d) Issuance of regulations and orders

The Board and the appropriate Federal banking agencies are authorized to issue such regulations and orders as may be necessary to enable them to administer and to carry out the purposes of this chapter and to prevent evasion thereof.

fulfill commitments entered into by the subsidiaries with third parties, if the bank holding company or servicing company complies with the Board's published interpretations and does not act as principal in dealing with third parties; and

- (2) The internal operations of the bank holding company or its subsidiaries. Services for the internal operations of the bank holding company or its subsidiaries include, but are not limited to: (i) accounting, auditing, and appraising; (ii) advertising and public relations; (iii) data processing and data transmission services, data bases or facilities; (iv) personnel services (v) courier services; (vi) holding or operating property used wholly or substantially by a subsidiary in its operations or for its future use; (vii) liquidating property acquired from a subsidiary; (viii) liquidating property acquired from any sources either prior to May 9, 1956, or the date on which the company became a bank holding company, whichever is later; and (ix) selling, purchasing, or underwriting insurance such as blanket bond insurance, group insurance for employees and property and casualty insurance. ...

Bank Holding Companies

Regulation Y (as amended February 12, 1990)

Subpart C – Nonbanking Activities and Acquisitions by Bank Holding Companies.

12 CFR 225.22 Exempt Nonbanking Activities and Acquisitions.

- (a) Servicing activities. A bank holding company may, without the Board's prior approval under this subpart, furnish services to or perform services for, or establish or acquire a company that engages solely in furnishing services to or performing services for:
 - (1) The bank holding company or its subsidiaries in connection with their activities as authorized by law, including services that are necessary to

Financial Institutions Reform, Recovery, and Enforcement Act of 1989

Title II - FDIC (12 USC 1811 et seq.)

Sec. 225. Contracts Between Depository Institutions and Persons Providing Goods, Products, or Services

The Federal Deposit Insurance Act (12 USC 1811 et seq.) is amended by inserting after section 29 (as added by section 224 of this title) the following new section:

"Sec. 30. Contract Between Depository Institutions And Persons Providing Goods, Products, Or Services.

"(a) IN GENERAL. – An insured depository institution may not enter into a written or oral contract with any person to provide goods, products, or services to or for the benefit of such

depository institution if the performance of such contract would adversely affect the safety or soundness of the institution.

"(b) RULEMAKING. – The Corporation shall prescribe such regulations and issue such orders, including definitions consistent with this section, as many be necessary to administer and carry out the purposes of, and prevent evasions of, this section.

"(c) ENFORCEMENT. – Any action taken by any appropriate Federal banking agency under section 8 to enforce compliance on the part of any insured depository institution with the requirements of this section may include a requirement that such institution properly reflect the transaction on its books and records.

"(d) NO PRIVATE RIGHT OF ACTION. – This section may not be construed as creating any private right of action.

"(e) STUDY. –

"(1) IN GENERAL. – The Attorney General and the Comptroller General of the United States shall jointly conduct a study on the extent to which –

"(A) insured depository institutions are entering into contracts with vendors under which vendors agree to purchase stock or assets from insured depository institutions or to invest capital in or make deposits in such institutions; and

"(B) if such practices occur, the extent to which such practices are having an anticompetitive effect and should be prohibited.

"(2) REPORT TO CONGRESS. – Before the end of the 1-year period beginning on the date of the enactment of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989, the Attorney General and the Comptroller General shall submit a report to the Congress on the results of the study conducted pursuant to paragraph (1)."

FDIC Improvement Act of 1991

On December 19, 1991, the FDIC Improvement Act (FDICIA) was signed into law, creating major changes in the regulation and supervision of insured depository institutions. Section 112 of FDICIA, entitled "Independent Annual Audits of Insured Depository Institutions" added section 36 to the Federal Deposit Insurance (FDI) Act. It established new audit, reporting, and audit committee requirements for certain insured depository institutions. FDIC regulation Part 363 implemented the new statutory requirements contained in section 36 of the FDI Act. Amendments to Part 363, adopted February 6, 1996 and became effective for fiscal years ending after March 31, 1996 are included.

Part 363 – Annual Independent Audits and Reporting Requirements

Sec.

363.0 OMB control number.

363.1 Scope.

363.2 Annual reporting requirements.

363.3 Independent public accountant.

363.4 Filing and notice requirements.

363.5 Audit committees.

Appendix A to Part 363 – Guidelines and Interpretations

Authority: 12 USC 1831m.

Source: The provisions of this Part 363 appear at 58 Fed. Reg. 31335, June 2, 1993, effective July 2, 1993, and 61 Fed. Reg. 6493, February 21, 1996 effective April 1, 1996..

363.0 OMB control number.

The collecting of information requirements in this part have been approved by the Office of Management and Budget under OMB control number 3064-0113.

363.1 Scope.

(a) *Applicability.* This part applies with respect to fiscal years of insured depository institutions which begin after December 31, 1992. This part does not

apply with respect to any fiscal year of any insured depository institution, the total assets of which, at the beginning of such fiscal year, are less than \$500 million.

(b) *Compliance by subsidiaries of holding companies.*

(1) The audited financial statements requirement of Section 363.2(a) may be satisfied for an insured depository institution that is a subsidiary of a holding company by audited financial statements of the consolidated holding company.

(2) The other requirements of this part for an insured depository institution that is a subsidiary of a holding company may be satisfied by the holding company if:

(i) The services and functions comparable to those required of the insured depository institution by this part are provided at the holding company level; and

(ii) The insured depository institution has as of the beginning of its fiscal year:

(A) Total assets of less than \$5 billion; or

(B) Total assets of \$5 billion or more and a composite CAMEL rating of 1 or 2.

(3) The appropriate federal banking agency may revoke the exception in paragraph (b)(2) of this section for any institution with total assets in excess of \$9 billion for any period of time during which the appropriate federal banking agency determines that the institution's exemption would create a significant risk to the affected deposit insurance fund.

363.2 Annual reporting requirements.

(a) *Audited financial statements.* Each insured depository institution shall prepare annual financial statements in accordance with generally accepted accounting principles which shall be audited by an independent public accountant.

(b) *Management report.* Each insured depository institution annually shall prepare, as of the end of the institution's most recent fiscal year, a management report signed by its chief executive

officer and chief accounting or chief financial officer which contains:

(1) A statement of management's responsibilities for preparing the institution's annual financial statements, for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and for complying with laws and regulations relating to safety and soundness which are designated by the FDIC and the appropriate federal banking agency; and

(2) Assessments by management of the effectiveness of such internal control structure and procedures as of the end of such fiscal year and the institution's compliance with such laws and regulations during such fiscal year.

363.3 Independent public accountant.

(a) *Annual audit of financial statement.* Each insured depository institution shall engage an independent public accountant to audit and report on its annual financial statements in accordance with generally accepted auditing standards and section 37 of the Federal Deposit Insurance Act (12 USC 1831n). The scope of the audit engagement shall be sufficient to permit such accountant to determine and report whether the financial statements are presented fairly and in accordance with generally accepted accounting principles.

(b) *Additional reports.* Such independent public accountant shall examine, attest to, and report separately on, the assertions of management concerning the institution's internal control structure and procedures for financial reporting. The accountant shall apply procedures agreed upon by the FDIC objectively to determine compliance by an insured depository institution with designated laws and regulations. The attestations shall be made in accordance with generally accepted standards for attestation engagements.

(c) *Notice by accountant of termination of services.* An independent public accountant performing an audit under this part who ceases to be the accountant for an insured depository institution shall notify the FDIC and the appropriate federal banking agency in writing of such termination within 15 days after the occurrence of such

event, and set forth in reasonable detail the reasons for such termination.

363.4 Filing and notice requirements.

- (a) *Annual reporting.* Within 90 days after the end of its fiscal year, each insured depository institution shall file with each of the FDIC, the appropriate federal banking agency, and any appropriate state bank supervisor, two copies of:
- (1) An annual report containing audited annual financial statements, the independent public accountant's report thereon, management's statements and assessments, and the independent public accountant's attestation report concerning the institution's internal control structure and procedures for financial reporting as required by Sections 363.2(a) and 363.3(a), 363.2(b), and 363.3(b) respectively; and
 - (2) The accountant's attestation concerning compliance with laws and regulations pursuant to Section 363.3(b).
- (b) *Public availability.* The annual report in paragraph (a)(1) of this section shall be available for public inspection.
- (c) *Independent accountant's reports.* Each insured depository institution shall file with the FDIC, the appropriate federal banking agency, and any appropriate state bank supervisor, a copy of any management letter, qualification, or other report issued by its independent public accountant with respect to such institution and the services provided by such accountant pursuant to this part within 15 days after receipt.
- (d) *Notice of engagement or change of accountants.* Each insured depository institution shall provide, within 15 days after the occurrence of any such event, written notice to the FDIC, the appropriate federal banking agency, and any appropriate state bank supervisor of the engagement of an independent public accountant, or the resignation or dismissal of the independent public accountant previously engaged. The notice shall include a statement of the reasons for any such event in reasonable detail.

363.5 Audit committees.

- (a) *Composition and duties.* Each insured depository institution shall establish an independent audit committee of its board of directors, the members of which shall be outside directors who are independent of management of the institution, and the duties of which shall include reviewing with management and the independent public accountant the basis for the reports issued under this part.
- (b) *Committees of large institutions.* The audit committee of any insured depository institution that has total assets of more than \$3 billion, measured as of the beginning of each fiscal year, shall include members with banking or related financial management expertise, have access to its own outside counsel, and not include any large customers of the institution. If a large institution is a subsidiary of a holding company and relies on the audit committee of the holding company to comply with this rule, the holding company audit committee shall not include any members who are large customers of the subsidiary institution.

Appendix A to Part 363 – Guidelines and Interpretations

Table of Contents

Introduction

Scope of Rule (363.1)

1. Measuring Total Assets
2. Insured Branches of Foreign Banks
3. Compliance by Holding Company Subsidiaries
4. Comparable Services and Functions

Annual Reporting Requirements (363.2)

5. Annual Financial Statements
6. Holding Company Statements
7. Insured Branches of Foreign Banks
8. Management Report
9. Safeguarding of Assets
10. Standards for Internal Controls
11. Service Organizations
12. Compliance with Laws and Regulations

Role of Independent Public Accountant (363.3)

13. General Qualifications
14. Independence
15. Peer Reviews
16. Filing Peer Review Reports
17. Information to Independent Public Accountant
18. Attestation Reports
19. Procedures for Determining Compliance with

-
- Designated Laws
 - 20. Reviews with Audit Committee and Management
 - 21. Notice of Termination
 - 22. Reliance on Internal Auditors
 - Filing and Notice Requirements (363.4)
 - 23. Place for Filing
 - 24. Relief From Filing Deadlines
 - 25. Public Availability
 - 26. Independent Public Accountant's Reports
 - 27. Notices Concerning Accountants
 - Audit Committees (363.5)*
 - 28. Composition
 - 29. "Independent of Management" Considerations
 - 30. Lack of Independence
 - 31. Holding Company Audit Committees
 - 32. Duties
 - 33. Banking or Related Financial Management Expertise
 - 34. Large Customers
 - 35. Access to Counsel
 - 36. Forming and Restructuring Audit Committees
 - Other
 - 37. Modifications of Guidelines

Schedule A to Appendix A – Agreed Upon Procedures for Determining Compliance with Designated Laws

Introduction

Congress added section 36, "Early Identification of Needed Improvements in Financial Management" (section 36), to the Federal Deposit Insurance Act (FDI Act) as part of the Federal Deposit Insurance Improvement Act of 1991, which became law on December 19, 1991.

The FDIC adopted 12 CFR Part 363 of its rules and regulations (this part), effective July 2, 1993, to implement those provisions of section 36 that require rulemaking. Simultaneously, the FDIC Board of Directors approved these "Guidelines and Interpretations" (the Guidelines) and directed that they be published as an appendix to this part to facilitate a better understanding of, and full compliance with, the provisions of section 36.

The Guidelines were developed by the FDIC, in consultation with the other appropriate federal banking agencies, after careful consideration of the comments received on the proposed rule.

Although not contained in this part, some of the guidance offered restates or refers to statutory

requirements of section 36 and is therefore mandatory. If that is the case, the statutory provision is cited. The FDIC continues to believe, as stated in its "Statement of Policy Regarding Independent External Auditing Programs of State Nonmember Banks" (Nov. 16, 1988), that every insured depository institution, regardless of its size or charter, should have an annual audit of its financial statements performed by an independent public accountant, and should establish an audit committee comprised entirely of outside directors.

The following Guidelines reflect the views of the FDIC concerning the interpretation of section 36. The Guidelines are intended to assist insured depository institutions (institutions), their boards of directors, and their advisors, including their independent public accountants and legal counsel, and to clarify section 36 and this part. It is recognized that reliance on the Guidelines may result in compliance with section 36 and this part which may vary from institution to institution. Terms which are not explained in the Guidelines have the meanings given them in this part, the FDI Act or professional accounting and auditing literature.

Scope of Rule (363.1)

1. *Measuring Total Assets.* To determine whether this part applies, an institution should use total assets as reported on its most recent Report of Condition (Call Report) or Thrift Financial Report (TFR), the date of which coincides with the end of its preceding fiscal year. If its fiscal year ends on a date other than the end of a calendar quarter, it should use its Call Report or TFR for the quarter end immediately preceding the end of its fiscal year.
2. *Insured Branches of Foreign Banks.* Unlike other institutions, insured branches of foreign banks are not separately incorporated or capitalized. To determine whether this part applies, an insured branch should measure claims on non-related parties reported on its Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks (form FFIEC 002).
3. *Compliance by Holding Company Subsidiaries.* Audited consolidated financial statements and other reports or notices required by this part which are submitted by a holding company for any subsidiary institution, should be

accompanied by a cover letter identifying all subsidiary institutions to which they pertain. An institution filing holding company consolidated financial statements as permitted by Section 363.1(b) also may report on changes in its independent public accountant on a holding company basis. An institution that does not meet the criteria in section 36(i) must satisfy the remaining provisions of the statute and this part on an individual institution basis, and maintain its own audit committee. Multi-tiered holding companies may satisfy all requirements of this part at any level.

4. *Comparable Services and Functions.* Services and functions will be considered "comparable" to those required by this part if the holding company:
 - (a) Prepares reports used by the subsidiary institution to meet the requirements of this part;
 - (b) Has an audit committee that meets the requirements of this part appropriate to its largest subsidiary institution; and
 - (c) Prepares and submits the management assessments of the effectiveness of the internal control structure and procedures for financial reporting (internal controls), and compliance with the Designated Laws defined in guideline 12 based on information concerning the relevant activities and operations of those subsidiary institutions within the scope of the rule.

Annual Reporting Requirements (363.2)

5. *Annual Financial Statements.* Each institution should prepare comparative annual consolidated financial statements (balance sheets, statements of income, changes in equity capital, and cash flows, with accompanying footnote disclosures) in accordance with generally accepted accounting principles (GAAP) for each of its two most recent fiscal years. Statements for the earlier year may be presented on an unaudited basis if the institution was not subject to this part for that year and audited statements were not prepared.
6. *Holding Company Statements.* Subsidiary institutions may file copies of their holding

company's audited financial statements filed with the Securities and Exchange Commission (SEC) or prepared for their FR Y-6 Annual Report under the Bank Holding Company Act of 1956.

7. *Insured Branches of Foreign Banks.* An insured branch of a foreign bank should satisfy the financial statements /requirement by filing one of the following for the two preceding fiscal years:
 - (a) Audited balance sheets, disclosing information about financial instruments with off-balance-sheet risk;
 - (b) Schedules RAL and L of form FFIEC 002, prepared and audited on the basis of the instructions for its preparation; or
 - (c) With written approval of the appropriate federal banking agency, consolidated financial statements of the parent bank.
8. *Management Report.* Management should perform its own investigation and review of the effectiveness of internal controls and compliance with the Designated Laws defined in guideline 12. Management also should maintain records of its determinations and assessments until the next federal safety and soundness examination, or such later date as specified by the FDIC or appropriate federal banking agency. Management should provide in its assessment of the effectiveness of internal controls and compliance with the Designated

Laws, or supplementally, sufficient information to enable the accountant to report on its assertions. The management report of an insured branch of a foreign bank should be signed by the branch's managing official if the branch does not have a chief executive or financial officer.

9. *Safeguarding of Assets.* "Safeguarding of assets", as the term relates to internal control policies and procedures regarding financial reporting, and which has precedent in accounting literature, should be encompassed in the management report and the independent public accountant's attestation discussed in guideline 18. Testing the existence of and compliance with internal controls on the management of assets, including loan underwriting and documentation,

represents a reasonable implementation of section 36. The FDIC expects such internal controls to be encompassed by the assertion in the management report, but the term "safeguarding of assets" need not be specifically stated. The FDIC does not require the accountant to attest to the adequacy of safeguards, but does require the accountant to determine whether safeguarding policies exist.²

10. *Standards for Internal Controls.*³ Each institution should determine its own standards for establishing, maintaining and assessing the effectiveness of its internal controls.
11. *Service Organizations.* Although service organizations should be considered in determining if internal controls are adequate, an institution's independent public accountant, its management, and its audit committee should exercise independent judgment concerning that determination. Onsite reviews of service organizations may not be necessary to prepare the reports required by the Rule, and the FDIC does not intend that the Rule establish any such requirement.
12. *Compliance with Laws and Regulations.* The designated laws and regulations are the federal laws and regulations concerning loans to insiders and the federal and state laws and regulations concerning dividend restrictions, which are more specifically identified in section 1 of the Agreed Upon Procedures referred to in guideline 19 (the Designated Laws).

² It is management's responsibility to establish policies concerning underwriting and asset management and to make credit decisions. The auditor's role is to test compliance with management's policies relating to financial reporting.

³ In considering what information is needed on safeguarding of assets and standards for internal controls, management may review guidelines provided by its primary federal regulator; the Federal Financial Institutions Examination Council's "Supervisory Policy Statement on Securities Activities"; the FDIC's "Statement of Policy Providing Guidance on External Auditing Procedure for State Nonmember Banks" (Jan. 16, 1990), "Statement of Policy Regarding Independent External Auditing Programs of State Nonmember Banks" (Nov. 16, 1988), and Division of Supervision Manual of Examination Policies; the Federal Reserve Board's Commercial Bank Examination Manual and other relevant regulations; the Office of Thrift Supervision's Thrift Activities Handbook; the Comptroller of the Currency's Handbook for National Bank Examiners; standards published by professional accounting organizations, such as the American Institute of Certified Public Accountant's (AICPA) Statement of Auditing Standards No. 55, "Consideration of the Internal Control Structure in a Financial Statement Audit"; the Committee of Sponsoring Organizations (COSO) of the Treadway Commission's Internal Control-Integrated Framework, including its addendum on safeguarding of assets; and other internal control standards published by the AICPA, other accounting or auditing professional associations, and financial institution trade associations.

Role of Independent Public Accountant (363.3)

13. *General Qualifications.* To provide audit and attest services to insured depository institutions, an independent public accountant should be registered or licensed to practice as a public accountant, and be in good standing, under the laws of the state or other political subdivision of the United States in which the home office of the institution (or the insured branch of a foreign bank) is located. As required by section 36(g)3(A)(i), the accountant must agree to provide copies of any work papers, policies, and procedures relating to services performed under this part.
14. *Independence.* The independent public accountant also should be in compliance with the AICPA's Code of Professional Conduct and meet the independence requirements and interpretations of the SEC and its staff.
15. *Peer Reviews.* As required by section 36(g)3(A)(ii), the independent public accountant must have received, or be enrolled in, a peer review that meets acceptable guidelines. The following peer review guidelines are acceptable:
 - (a) The external peer review should be conducted by an organization independent of the accountant or firm being reviewed, as frequently as is consistent with professional accounting practices;
 - (b) The peer review should be generally consistent with AICPA standards;⁴ and
 - (c) The review should include, if available, at least one audit on an insured depository institution or consolidated financial holding company. Peer review working papers are to be retained for 120 days after the peer review report is filed with the FDIC, and be made available to the FDIC upon request, in a form consistent with the SEC's agreement with the accounting profession.
16. *Filing Peer Review Reports.* Within 15 days of receiving notification that the peer review has

⁴ These would include Standards for Performing and Reporting on Peer Reviews, codified in the *SEC Practice Section Reference Manual*, and Standards for Performing and Reporting on Quality Reviews, contained in Volume 2 of the AICPA's *Professional Standards*.

been accepted, or before commencing any audit under this part, whichever is earlier, two copies of the peer review report, accompanied by any letter of comments and letter of response, should be filed by the independent public accountant with the FDIC, Registration and Disclosure Section, 550 17th Street N.W., Washington, D.C. 20429, where they will be available for public inspection. Accountants may elect to file an annual list of their insured depository institution and holding company (identifying any subsidiary institutions subject to this part) audit clients in lieu of copies of peer review reports for each institution they have been engaged to audit. The FDIC has determined that such client lists are exempt from public disclosure. All corrective action required under any qualified peer review report should have been taken prior to commencing services under this part.

17. *Information to Independent Public Accountant.* Attention is directed to section 36(h) which requires institutions to provide specified information to their accountants. An institution also should provide its accountant with copies of any notice that the institution's capital category is being changed or reclassified under section 38 of the FDI Act, and any correspondence from the appropriate federal banking agency concerning compliance with this part.
18. *Attestation Reports.* The independent public accountant should provide the institution with an internal controls attestation report, a compliance with Designated Laws attestation report, and any management letter, at the conclusion of the audit as required by section 36(c)(1). If a holding company subsidiary relies on its holding company management report, the accountant may attest to and report on the management's assertions in one report, without reporting separately on each subsidiary covered by this part. One attestation report for compliance with the designated laws also may be filed, if all exceptions are listed and the respective institutions to which the exceptions apply are identified. The FDIC has determined that management letters and the Designated Laws attestation report are exempt from public disclosure.
19. *Procedures for Determining Compliance with Designated Laws.* In order to permit the independent public accountant to determine the

extent of compliance with the Designated Laws defined in guideline 12 and the related assessment by management, the procedures set forth in schedule A (the Agreed Upon Procedures) to these Guidelines in this appendix should be applied. The accountant should require all management representations to be in writing, and take appropriate steps to determine that any sampling is reasonably representative. Attestation reports generally should identify all findings from application of the Agreed Upon Procedures which establish any items of non-compliance, note any absence of written policies, and disclose the reasons why any Agreed Upon Procedures were not performed.

20. *Reviews with Audit Committee and Management.* The independent public accountant should meet with the institution's audit committee to review the accountant's reports required by this part before they are filed. It also may be appropriate for the accountant to review its findings with the institution's board of directors and management.
21. *Notice of Termination.* The notice required by 363.3(c) should state whether the independent public accountant agrees with the assertions contained in any notice filed by the institution under Section 363.4(d), and whether the institution's notice discloses all relevant reasons.
22. *Reliance on Internal Auditors.* Nothing in this part or this appendix is intended to preclude the ability of the independent public accountant to rely on the work of an institution's internal auditor.

Filing and Notice Requirements (363.4)

23. *Place for Filing.* Except for peer review reports filed pursuant to Guideline 16, all reports and notices required by, and other communications or requests made pursuant to, this part should be filed as follows:
 - (a) FDIC: Regional Director (Supervision) of the FDIC Regional Office in which the institution is headquartered;
 - (b) Office of the Comptroller of the Currency (OCC): appropriate OCC Supervisory Office;

-
- (c) Federal Reserve: appropriate Federal Reserve Bank;
 - (d) Office of Thrift Supervision (OTS): appropriate OTS District Office; and
 - (e) State bank supervisor: the filing office of the appropriate state bank supervisor.

24. *Relief from Filing Deadlines.* Although the reasonable deadlines for filings and other notices established by this part are specified, some institutions may occasionally be confronted with extraordinary circumstances beyond their reasonable control that may justify extensions of a deadline. In that event, upon written application from an insured depository institution, setting forth the reasons for a requested extension, the FDIC or appropriate federal banking agency may, for good cause, extend a deadline in this part for a period not to exceed 30 days.

25. *Public Availability.* Each institution's annual report should be available for public inspection at its main and branch offices no later than 15 days after it is filed with the FDIC. Alternatively, an institution may elect to mail one copy of its annual report to any person who requests it. The annual report should remain available to the public until the annual report for the next year is available. An institution may use its annual report under this part to meet the annual disclosure statement required by 12 CFR 350.3, if the institution satisfies all other requirements of 12 CFR Part 350.

26. *Independent Public Accountant's Reports.* Section 36(h)(2)(A) requires that, within 15 days of receipt by an institution of any management letter or other report, such letter or other report shall be filed with the FDIC, any appropriate federal banking agency, and any appropriate state bank supervisor. Institutions and their accountants are encouraged to coordinate preparation and delivery of audit and attestation reports and filing the annual report, to avoid duplicate filings.

27. *Notices Concerning Accountants.* Institutions should review and satisfy themselves as to compliance with the required qualifications set forth in guidelines 13-15 before engaging an independent public accountant. With respect to

any selection, change or termination of an accountant, institutions should be familiar with the notice requirements in guideline 21, and should send a copy of any notice under Section 363.4(d) to the accountant when it is filed with the FDIC. An institution which files reports with its appropriate federal banking agency under, or is a subsidiary of a holding company which files reports with the SEC pursuant to, the Securities Exchange Act of 1934 may use its current report (e.g., SEC Form 8-K) concerning a change in accountant to satisfy the similar notice requirements of this part.

Audit Committees (363.5)

28. *Composition.* The board of directors of each institution should determine if outside directors meet the requirements of section 36 and this part. At least annually, it should determine whether all existing and potential audit committee members are "independent of management of the institution." If the institution has total assets in excess of \$3 billion, the board also should determine whether members of the committee satisfy the additional requirements of this part. Because an insured branch of a foreign bank does not have a separate board of directors, the FDIC will not apply the audit committee requirements to such branch. However, any such branch is encouraged to make a reasonable good faith effort to see that similar duties are performed by persons whose experience is generally consistent with the Rule's requirements for an institution the size of the insured branch.

29. *"Independent of Management" Considerations.* In determining whether an outside director is independent of management, the board should consider all relevant information. This would include considering whether the director:

- (a) Is or has been an officer or employee of the institution or its affiliates;
- (b) Serves or served as a consultant, advisor, promoter, underwriter, legal counsel, or trustee of or to the institution or its affiliates;
- (c) Is a relative of an officer or other employee of the institution or its affiliates;
- (d) Holds or controls, or has held or controlled,

-
- a direct or indirect financial interest in the institution or its affiliates; and (e) Has outstanding extensions of credit from the institution or its affiliates.
30. *Lack of Independence.* An outside director should not be considered independent of management if such director is, or has been within the preceding year, an officer or employee of the institution or any affiliate, or owns or controls, or has owned or controlled within the preceding year, assets representing 10 percent or more of any outstanding class of voting securities of the institution.
31. *Holding Company Audit Committees.* When an insured depository institution subsidiary fails to meet the requirements for the holding company exception in Section 363.1(b)(2) or maintains its own separate audit committee to satisfy the requirements of this part, members of the independent audit committee of the holding company may serve as the audit committee of the subsidiary institution if they are otherwise independent of management of the subsidiary, and, if applicable, meet any other requirements for a large subsidiary institution covered by this part. However, this does not permit officers or employees of a holding company to serve on the audit committee of its subsidiary institutions. When the subsidiary institution satisfies the requirements for the holding company exception in Section 363.1(b)(2), members of the audit committee of the holding company should meet all the membership requirements applicable to the largest subsidiary depository institution and may perform all the duties of the audit committee of a subsidiary institution, even though such holding company directors are not directors of the institution.
32. *Duties.* The audit committee should perform all duties determined by the institution's board of directors. The duties should be appropriate to the size of the institution and the complexity of its operations, and include reviewing with management and the independent public accountant the basis for the reports issued under Sections 363.2(a) and (b) and 363.3(a) and (b). Appropriate additional duties could include:
- (a) Reviewing with management and the independent public accountant the scope of services required by the audit, significant accounting policies, and audit conclusions regarding significant accounting estimates;
 - (b) Reviewing with management and the accountant their assessments of the adequacy of internal controls, and the resolution of identified material weaknesses and reportable conditions in internal controls, including the prevention or detection of management override or compromise of the internal control system;
 - (c) Reviewing with management and the accountant the institution's compliance with laws and regulations;
 - (d) Discussing with management the selection and termination of the accountant and any significant disagreements between the accountant and management; and
 - (e) Overseeing the internal audit function. It is recommended that audit committees maintain minutes and other relevant records of their meetings and decisions.
33. *Banking or Related Financial Management Expertise.* At least two members of the audit committee of a large institution shall have "banking or related financial management expertise" as required by section 36(g)(1)(C)(i). This determination is to be made by the board of directors of the insured depository institution. A person will be considered to have such required expertise if the person has significant executive, professional, educational, or regulatory experience in financial, auditing, accounting, or banking matters as determined by the board of directors. Significant experience as an officer or member of the board of directors or audit committee of a financial services company would satisfy these criteria.
34. *Large Customers.* Any individual or entity (including a controlling person of any such entity) which, in the determination of the board of directors, has such significant direct or indirect credit or other relationships with the institution, the termination of which likely would materially and adversely affect the institution's financial condition or results of operations, should be considered a "large customer" for purposes of Section 363.5(b).

35. *Access to Counsel.* The audit committee should be able to retain counsel at its discretion without prior permission of the institution's board of directors or its management. Section 36 does not preclude advice from the institution's internal counsel or regular outside counsel. It also does not require retaining or consulting counsel, but if the committee elects to do either, it also may elect to consider issues affecting the counsel's independence. Such issues would include whether to retain or consult only counsel not concurrently representing the institution or any affiliate, and whether to place limitations on any counsel representing the institution concerning matters in which such counsel previously participated personally and substantially as outside counsel to the committee.

36. *Forming and Restructuring Audit Committees.* Audit committees should be formed within four months of the effective date of this part. Some institutions may have to restructure existing audit committees to comply with this part. No regulatory action will be taken if institutions restructure their audit committees by the earlier of their next annual meeting of stockholders, or one year from the effective date of this part.

Other

37. *Modifications of Guidelines.* The FDIC Board of Directors has delegated to the Director of the FDIC's Division of Supervision authority to make and publish in The Federal Register minor technical amendments to the Guidelines in this appendix (including the attached Agreed Upon Procedures in Schedule A to this appendix), in consultation with the other appropriate federal banking agencies, to reflect the practical experience gained from implementation of this part. It is not anticipated any such modification would be effective until affected institutions have been given reasonable advance notice of the modification. Any material modification or amendment will be subject to review and approval of the FDIC Board of Directors.

Schedule A to Appendix A – Agreed upon Procedures for Determining Compliance with Designated Laws

1. The Agreed Upon Procedures set forth in this schedule are referred to in guideline 19. They should be followed by the institution's independent public

accountant (or, with respect to the procedures set forth in section I of this schedule, by the institution's internal auditor if the accountant is to perform the procedures set forth in section II) in order to permit the accountant to report on the extent of compliance with the Designated Laws (defined in guideline 12) as required by sections 36(e)(1) and (2). Unless otherwise stated, the date of any required representation should be the same as the date of the attestation report and the representation should provide information to the extent available as of that date.

2. For purposes of this Schedule A, "insiders" means directors, executive officers, and principal shareholders, and includes their related interests. All terms not defined in this schedule have the meanings given them in this part, the Guidelines, and professional accounting and auditing literature.

3. Additional guidance concerning the role of the institution, its internal auditor, and its independent public accountant in assessing the institution's compliance with the Designated Laws is set forth in the Guidelines.

Section I – Procedures for Individual Institutions

The following procedures should be performed by the institution's independent public accountant in accordance with generally accepted standards for attestation engagements, or by the institution's internal auditor if the procedures set forth in section II of this schedule are to be performed by the independent public accountant. (See section II.B.3. for information concerning testing by the independent public accountant when the institution's internal auditor is performing the procedures in Section I.)

A. *Loans to Insiders.* To the extent permitted by §363.1(b)(2), these procedures may be performed on a holding company basis rather than at each covered subsidiary insured depository institution.

1. *Designated Laws.* The following federal laws and regulations (Designated Insider Laws), to the extent that they are applicable to the institution, should be read:

a. Laws: 12 USC 375a, 375b, 1468(b), 1828(j)(2), and 1828(j)(3)(B); and

b. Regulations: 12 CFR 23.5, 31, 215, 337.3, 349.3, and 563.43.

2. General.

a. Information. Obtain from management of the institution the following information for the institution's fiscal year:⁵

- (1) Management's assessment of compliance with the Designated Insider Laws;
- (2) All minutes (including minutes drafted, but not approved) of the meetings of the board and of those committees of the board which management represents have been delegated authority pertaining to insider lending;
- (3) The relevant portions of reports of examination, supervisory agreements, and enforcement actions issued by the institution's primary federal and state regulators, if applicable, which management represents contain information pertaining to insider lending;
- (4) The annual survey which identifies all insiders of the institution (pursuant to 12 CFR 215.8(b)) or other records maintained on insiders of the institution's affiliates (pursuant to 12 CFR 215.8(c));
- (5) The relevant portions of the following Securities Exchange Act of 1934 filings, which management represents contain information pertaining to insider lending:
 - (a) Forms 10-K, 10-Q, and 8-K and proxy statements (or information statements) filed with the SEC, Federal Reserve Board, OCC, or OTS, or
 - (b) Forms F-2, F-3, and F-4 and

proxy statements (or information statements), filed with the FDIC;

- (6) A list of loans, including overdrafts of executive officers and directors,⁶ and other extensions of credit to insiders (including their related interests) outstanding at any time during the fiscal year (and which identifies those extensions granted during the year). This list should also include the amount outstanding of each extension of credit as of the date of the most recently filed Call Report or TFR (Insider Extensions List); and
- (7) Management's representation concerning:
 - (a) The completeness of the Insider Extensions List;⁷ and
 - (b) The inclusion of all required insiders on the annual survey obtained in paragraph A.2.a.(4) of this section including persons who have been designated as executive officers by resolution of the board or a committee of the board or in the by-laws of the institution.

b. Procedures:

- (1) Read the foregoing information.
- (2) Trace and agree a sample of insider loans and other extensions of credit disclosed in the documents listed in paragraphs A.2.a.(2) through (5) of this section to see that they are included on the Insider Extensions List.

3. Policies and Procedures.

a. Information. Obtain the institution's written policies and procedures concerning its compliance with the Designated Insider Laws,

⁵ If the institution chooses to have these procedures performed using its most recently filed Call Report rather than its year end Call Report, all references to "fiscal year" in these procedures shall mean the period beginning with the latest Call Report date for which these procedures were performed in the prior year and ending with the date of the most recently filed Call Report. If these procedures were not previously performed, the 12 month period immediately preceding the date of the most recently filed Call Report (or such shorter period during which the institution was covered by this Part 363) should be used.

⁶ Management may exclude from this list overdrafts of an executive officer or director in an aggregate amount of \$1,000 or less without overdraft protection and those of \$5,000 or less with overdraft protection as specified in 12 CFR 215.3(b)(6) if management provides the independent accountant with a representation that policies and procedures are in effect to report as extensions of credit all overdrafts that do not meet the criteria listed in paragraphs A.8.a.(2)(a) through (c) of this section.

⁷ See footnote 6 of this schedule.

including any written "Code of Ethics" or "Conflict of Interest" policy statements. If the institution has no written policies and procedures, obtain a narrative from management that describes the methods for complying with such laws and regulations, and includes provisions similar to those listed in paragraph A.3.b. of this section.

b. Procedures. Ascertain that the policies and procedures include, or incorporate by reference, provisions consistent with the Designated Insider Laws for:

- (1) Defining terms;
- (2) Restricting loans to insiders;
- (3) Maintaining records of insider loans;
- (4) Requiring reports and/or disclosures by the institution and by executive officers, directors, and principal shareholders (and their related interests);
- (5) Disseminating policy information to employees and insiders; and
- (6) Prior approval of the board of directors.

4. Calculations of Lending Limits.

a. Information. Obtain management's calculation of the following items as of the date of the institution's most recently filed Call Report or TFR and as of a Call Report or TFR date six or nine months earlier:

- (1) The institution's unimpaired capital and surplus (the aggregate lending limit for all insiders); and
- (2) The institution's individual lending limit (12 CFR 215.2(i)).

b. Procedures. Recalculate the amounts in paragraph A.4.a. of this section for mathematical accuracy, and trace the amounts used in management's calculations to the Call Reports or TFRs for the two dates used in paragraph A.4.a. of this section.

5. Insider Extensions of Credit Granted.

a. Information. Obtain management's

representation regarding whether the terms and creditworthiness of insider extensions of credit granted during the fiscal year are comparable to those that would have been available to unaffiliated third parties.

b. Procedures. Select a sample of insiders who were granted or had outstanding extensions of credit during the fiscal year from the Insider Extensions List. For each extension of credit granted during the fiscal year to each insider in the sample selected:

(1) If the amount of a credit granted during the year (when aggregated with all other extensions of credit to that person and to all related interests of that person) exceeds \$ 500,000, determine whether the minutes of the meetings of the board of directors indicate that:

- (a) The credit was approved in advance by the board, and
- (b) The insider, if a director, abstained from participating directly or indirectly in voting on the transaction;

(2) Obtain management's calculation of the institution's individual lending limit for insiders pursuant to 12 CFR 215.2(i) as of the date of the Call Report or TFR filed immediately prior to the date when the extension of credit was granted, and if not already done under paragraph A.4.b. of this section, recalculate the lending limits for mathematical accuracy, and trace the amounts used in management's calculations to the Call Report or TFR for that date. Ascertain whether the amount of the extension of credit being granted to the insider, when combined with all other extensions of credit to that insider, exceeds such limit; and

(3) For one transaction involving each insider in the sample selected in paragraph A.5.b. of this section, perform the procedures in either paragraph (a) or (b) as follows:

- (a) Select three (or such smaller number that exists) similar extensions of credit (e.g., commercial real estate loans,

floor plan loans, residential mortgage loans, consumer loans) granted to unaffiliated borrowers (i.e., persons who are not insiders or employees of the institution or its affiliates) within 90 days before or after the granting of the insider extension of credit. Compare the terms of the transactions with unaffiliated borrowers (i.e., rate or range of interest rates, maturity, payment terms, collateral, and any unusual provisions or conditions) to those with the insiders, and note in the findings any differences in the terms favorable to the insiders compared to the terms of the transactions with unaffiliated borrowers.

- (b) Alternatively, compare the terms of each insider transaction in the sample to approved policies delineating the interest rate and other terms and conditions then in effect for similar extensions of credit to unaffiliated borrowers. Note in the findings any differences in the terms favorable to the insiders compared to the terms of the approved policies for an extension of credit to persons not affiliated with the institution or its affiliates.

6. Limitation on Extensions of Credit to Executive Officers.

a. Information. From the sample selected in paragraph A.5.b. of this section, select the executive officers who were granted extensions of credit during the fiscal year.

b. Procedures.

- (1) For each executive officer selected, obtain management's calculation as of the two dates used in paragraph A.4.a. of this section of:
 - (a) The aggregate amount of extensions of credit to the executive officer, and
 - (b) 2.5 percent of the institution's unimpaired capital and surplus.
- (2) Recalculate management's computations from paragraph A.6.b.(1) of this section for mathematical accuracy. Trace amounts used

in management's computations from paragraph A.6.b.(1) to the Call Reports or TFRs for the two dates used in paragraph A.4.a. of this section.

- (3) Ascertain whether the aggregate amount of the extensions of credit to the executive officer does not exceed the greater of \$ 25,000 or 2.5 percent of the institution's unimpaired capital and surplus, but in no event more than \$ 100,000. The aggregate amount should exclude the types of extensions of credit set forth in 12 CFR 215.5(c)(1) through (3).

- (4) (a) Obtain documentation for any credits for which management represents that:

- (i) The purpose is for the purchase, construction, maintenance, or improvement of the executive officer's residence;

- (ii) The credit is secured by a first lien on the residence; and

- (iii) The executive officer owns or expects to own the residence after the extension of credit.

- (b) Note whether the documentation contains similar representations.

- (5) For each executive officer selected, ascertain that each extension of credit granted during the fiscal year was:

- (a) Preceded by submission of financial statements;

- (b) Approved by, or, when appropriate, promptly reported to, the board of directors no later than the next board meeting; and

- (c) Made subject to the written condition that the extension of credit will become, at the option of the institution, due and payable at any time that the executive officer is indebted to other insured institutions in an aggregate amount greater than the executive officer would be able to borrow from

the institution.

7. Aggregate Insider Extensions of Credit Outstanding.

a. Information. Obtain management's calculation of the aggregate extensions of credit to executive officers, directors, and principal shareholders of the institution and to their related interests, excluding the types of extensions of credit set forth in 12 CFR 215.4(d)(3), as of the two dates selected in paragraph A.4.a. of this section.

b. Procedures.

(1) Recalculate the amounts obtained in paragraph A.7.a. of this section for mathematical accuracy and ascertain that this total, excluding the types of extensions of credit set forth in 12 CFR 215.4(d)(3), is less than or equal to 100 percent of the institution's unimpaired capital and surplus calculated in paragraph A.4.a.(1) of this section.

(2) Using the sample of insiders selected in paragraph A.5.b. of this section, trace and agree amounts outstanding from insiders in the sample to the supporting documents, as applicable, for the line item aggregating indebtedness of all insiders on the institution's most recently filed Call Report or TFR.

8. Overdrafts.

a. Information. Select a sample of executive officers and directors who had overdrafts outstanding during the fiscal year as shown on the Insider Extensions List.

(1) For all overdrafts in the sample except those which are covered by an overdraft protection line of credit with the same terms as available to unaffiliated borrowers and meet the terms of that overdraft protection line, obtain management's representation of the history of the insider's overdrafts for the year and the completeness of that history.

(2) If the institution's management has not provided a representation as specified by footnote 3 to paragraph A.2.a.(6) of this section, for each overdraft in the sample in

an aggregate amount of \$ 1,000 or less for an executive officer or director who did not have the overdraft covered by an overdraft protection line of credit, obtain management's representation that:

(a) It believes the overdraft was inadvertent;

(b) The account was overdrawn in each case for no more than 5 business days; and

(c) The institution charged the executive officer or director the same fee that it would charge any other customer in similar circumstances.

b. Procedures. For each overdraft in the sample selected and used in paragraph A.8.a.(1) of this section for which management did not provide the representation in paragraph A.8.a.(2) of this section:

(1) Inquire whether cash items for the insider were being held by the institution during the time that the overdraft was outstanding to prevent additional overdrafts;

(2) Trace and agree subsequent payment by the insider of the insider's overdrafts to records of the account at the institution; and

(3) For overdrafts of executive officers and directors that were paid by the institution for the executive officer or director from an account at the institution:

(a) Trace and agree to a written, pre-authorized, interest-bearing extension of credit plan that specifies a method of repayment; or

(b) Trace and agree to a written, pre-authorized transfer of funds from another account of the insider at the institution.

9. Reports on Indebtedness to Correspondent Banks.

a. Information. Obtain from management:

(1) A list of executive officers and principal shareholders and related interests thereof

that filed reports of indebtedness to a correspondent bank. This list should be prepared by management from reports of indebtedness submitted for the calendar year for which the management assessment and independent public accountant's attestation are being filed or, if the institution is on a calendar year fiscal year, at management's option, for the immediately preceding year. If the institution is not on a calendar year fiscal year, the list should be prepared for the calendar year that ended during its fiscal year; and

(2) Its representation concerning the completeness of the list prepared for paragraph A.9.a.(1) of this section.

b. Procedures. Select a sample of executive officers, principal shareholders, and related interests thereof from the list obtained in paragraph A.9.a.(1) of this section. For each executive officer and principal shareholder (or related interest thereof) included in the sample, ascertain that the report(s) of indebtedness was (were) filed with the board of directors (on or before the January 31 following the calendar year in paragraph A.9.a.(1) of this section) and that such report(s) state(s):

(1) The maximum amount of indebtedness during that calendar year;

(2) The amount of indebtedness outstanding 10 days prior to report filing; and

(3) A description of the loan terms and conditions, including the rate or range of interest rates, original amount and date, maturity date, payment terms, collateral, and any unusual terms or conditions.

B. Dividend Restrictions. If the institution has declared any dividends during the fiscal year, the following procedures should be performed for each dividend declared. (These procedures are not applicable to mutual institutions and insured branches of foreign banks.) For an institution that is a subsidiary of a holding company, the procedures that follow should be applied to each subsidiary institution subject to this part (covered subsidiary) because the laws and regulations restricting dividends apply to individual institutions and not holding

companies. However, if the annual report under Part 363 is being prepared on a holding company basis and the holding company has more than five covered subsidiaries, the following procedures may be applied to a sample of dividend declarations to the extent permitted by §363.1(b) and Section II.B.3. of this schedule.

1. Designated Laws. The following federal laws and regulations (Designated Dividend Laws), to the extent that they are applicable to the institution (see paragraph B.2 of this section),⁸ should be read:

a. Laws: 12 USC 56, 60, 1467a(f), 1831o; and

b. Regulations: 12 CFR 5.61, 5.62, 6.6, 7.6120, 208.19, 208.35, 325.105, 563.134, and 565.

2. General. The information requirements and procedures in paragraphs B.2. through B.5. of this section are applicable to all institutions. Paragraphs B.6. and B.7. of this section were designed to be applicable to member banks (i.e., national banks and state member banks) and federally-chartered savings associations, respectively. However, the requirements in paragraphs B.6. and B.7. of this section should be applied to a state nonmember bank or state savings association if management represents that the state has dividend restrictions substantially identical to those for a national bank or a federally-chartered savings association.

a. Information. Obtain from management of the institution the following information for the institution's most recent fiscal year:

(1) Its assessment of the institution's compliance with the Designated Dividend Laws and any applicable state laws and regulations cited in its assessment;

(2) A copy of any supervisory agreements with, orders by, or resolutions of any regulatory agency (including a description of the nature of any such agreements, orders, or resolutions) containing restrictions on dividend payments by the institution; and

(3) Its representation whether dividends

⁸The laws and regulations applicable to each type of institution are listed in Table 1 of this Schedule A to Appendix A.

declared comply with any restrictions on dividend payments under any supervisory agreements with, orders by, or resolutions of any regulatory agency (including a description of the nature of any such agreements, orders, or resolutions).

b. Procedures.

- (1) Read the foregoing information.
- (2) If any restrictions on dividend payments exist in any documents obtained in paragraph B.2.a.(2) of this section, test and agree dividends declared with any such quantitative restrictions.

3. Policies and Procedures.

- a. Information. Obtain the institution's written policies and procedures concerning its compliance with the Designated Dividend Laws. If the institution has no written policies and procedures, obtain from the institution a narrative that describes the institution's methods for complying with the Designated Dividend Laws, and includes provisions similar to those in paragraph B.3.b of this section.
- b. Procedures. Ascertain whether the policies and procedures include, or incorporate by reference, provisions which are consistent with the Designated Dividend Laws. These would include capital limitation tests, including section 38 of the Federal Deposit Insurance Act (12 USC 1831o), earnings limitation tests, transfers from surplus to undivided profits, and restrictions imposed under any supervisory agreements, resolutions, or orders of any federal or state depository institution regulatory agency. In addition, for savings associations, this would include prior notification to the OTS.

4. Board Minutes.

- a. Information. Obtain the minutes of the meetings of the board of directors for the most recent fiscal year to ascertain whether dividends (either paid or unpaid) have been declared.
- b. Procedures. Trace and agree total dividend amounts to the general ledger records and the institution's most recently filed Call Report or

TFR.

5. Calculation of Undercapitalization.

- a. Information. Obtain management's computation of the amount at which declaration of a dividend would cause the institution to be undercapitalized as of the quarter end (or more recent month end, if available from management) immediately prior to the date on which each dividend was declared during the fiscal year.
- b. Procedures. Recalculate management's computation (for mathematical accuracy) and compare management's calculations to the amount of any dividend declared to determine whether it exceeded the amount.

6. Dividends Declared by Banks.

- a. Information. If the institution is a national bank or state member bank, obtain management's computations concerning the bank's compliance with 12 USC 56, "Capital Limitation Test", 12 USC 60, "The Earnings Limitation Test", and transfers from surplus to undivided profits after declaration of the dividends referenced in paragraph B.4.a. of this section. If the institution is a state nonmember bank and management represents that the bank is subject to state laws that are similar to 12 USC 56 and 12 USC 60, obtain management's corresponding computations.
- b. Procedures. Recalculate management's computations (for mathematical accuracy) and compare management's calculations to the standards defined in the tests set forth in paragraph B.6.a. of this section to ascertain whether the dividends declared fall within the permissible levels under these standards. If dividends are not permissible in the amounts declared under such standards, the independent public accountant should ascertain that the dividends were declared with the approval of the appropriate federal banking agency or under any other exception to the standards.

7. Dividends Declared by Savings Associations.

- a. Information. Obtain management's documentation of the OTS determination

whether the institution is a Tier 1, Tier 2, or Tier 3 savings association and management's computations of its capital ratio after declarations of dividends under the Tier determined by the OTS. For dividends declared, obtain copies of the savings association's notifications to the OTS to ascertain whether notifications were made at least 30 days before payment of any dividends.

- b. Procedures. Recalculate management's computations (for mathematical accuracy) and trace amounts used by management in its calculations to the institution's TFRs.

Section II – Procedures for Independent Public Accountant

If the internal auditor has performed the procedures set forth in section I for either or both Designated Laws, the following procedures may be performed by the independent public accountant if neither the FDIC nor the appropriate federal banking agency has objected in writing. The report of procedures performed and list of exceptions found by the internal auditor, identifying the institution with respect to which any exception was found, should be submitted to the audit committee of the board of directors. Management should file a summary of the internal auditor's findings and management's response to those findings with the FDIC and the appropriate federal banking agency at the same time as the independent public accountant's attestation report is filed.⁹

- A. Review of Section I Procedures. Read the portion(s) of Section I of this schedule that set forth the procedures performed by the internal auditors.
- B. Information and Procedures. Perform the following procedures:
1. Designated Laws. Read the Designated Laws referred to in Section I of this schedule for the agreed-upon procedures performed by the internal auditor. Obtain management's assessment contained in its management report on the institution's or holding company's

compliance with the Designated Laws.

2. Internal Auditor's Workpapers.

- a. Information. If an internal auditor performed the procedures in Section I, obtain the internal auditor's workpapers documenting the performance of those procedures on the institution and the chief internal auditor's representation that:

- (1) The internal auditor or audit staff, if applicable, performed the procedures listed in section I on the institution;
- (2) The internal auditor tested a sufficient number of transactions governed by the Designated Laws so that the testing was representative of the institution's volume of transactions;
- (3) The workpapers accurately reflect the work performed by the internal auditor and, if applicable, the internal audit staff;
- (4) The workpapers obtained are complete; and
- (5) The internal auditor's report, which describes the procedures performed for the fiscal year as well as the internal auditor's findings and exceptions noted, has been presented to the institution's audit committee.

b. Procedures.

- (1) Compare the workpapers to the procedures that are required to be performed under section I. Report as an exception any procedures not documented and any procedures for which the sample size is not sufficient.
- (2) Compare the exceptions and errors listed by the internal auditor in its report to the audit committee to those found in the workpapers, and report as an exception any exception or error found in the internal auditor's workpapers and not listed in the internal auditor's list of exceptions.

3. Testing.

- a. The independent public accountant should

⁹ Since this summary provides information similar to that provided in the independent public accountant's report, the FDIC has determined that the summary is exempt from public disclosure consistent with the guidance in Guideline 18 in Appendix A to this Part 363.

perform the procedures listed in Section I on representative samples of the insiders and/or transactions of the institution to which the Designated Law applies. If the institution's internal auditor performs the procedures in Section I, the samples tested by the independent public accountant should be at least 25 percent of the size of the samples tested by the internal auditor although samples selected by the accountant should be from the population at large. However, if there are so few transactions in any area that the internal auditor cannot use sampling, but must test all transactions, the independent public accountant should also test all transactions.

- b. If testing under this Schedule A to Appendix A is being performed on a holding company with more than one subsidiary institution that is subject to this Part 363, the samples tested should include a combination of insiders and transactions from each covered subsidiary with

total assets (after deductions of intercompany amounts that would be eliminated in consolidation) in excess of 25 percent of the holding company's total assets every fiscal year. Samples should be tested for each smaller covered subsidiary at least every other fiscal year unless the holding company has more than eight covered subsidiaries, in which case the samples to be tested for each Designated Law should be drawn from each smaller covered subsidiary at least every third fiscal year.

- 4. Reports Concerning Holding Companies. Only one report of any exceptions noted from application of the procedures in section II performed by the independent public accountant should be filed as required by guideline 3 in Appendix A to this Part 363, but the report should identify, for each exception or error noted, the identity of the covered subsidiary to which it relates.

Tables to Schedule A to Appendix A Table 1

For engagements involving management assertions about compliance by:

Loans to insiders	National Banks	State mem- ber banks	State nonmember banks	Savings associations
Read the following parts and/or sections of Title 12 of the United States Code:				
375a	Loans to Executive Officers of	✓	✓	✓ <i>Subsections (g) And (h) only</i>
375b	Prohibitions Respecting Loans and Extensions of Credit to Executive Officers and Directors of Banks, Political Campaign, Committees, etc	✓	✓	
1468(b)	Extensions of Credit to Executive Officers, Directors, and Principal Shareholders			✓
1828(j)(2)	Provisions Relating to Loans, Extensions of Credit, and Other Dealings Between Member Banks and Their Affiliates, Executive Officers, Directors, etc			✓
1828(j)(3)(B)	Extensions of Credit Applicability of Provisions Relating to Loans, Extensions of Credit and Other Dealings Between Insured Branches of Foreign Banks and Their Insiders	✓ <i>Applies only</i>	✓ <i>Applies only to insured</i>	✓ <i>Applies only to state branches of foreign banks</i>
Read the following parts and/or sections of Title 12 of the Code of Federal Regulations:				
23.5	Application of Legal Lending Limits; Restrictions on Transactions With Affiliates		✓	
31	Extensions of Credit to National Bank Insiders	✓		
215 <i>CFR</i>	Subpart A – Loans by Member Banks to their Executive Officers, Directors, and Principal Shareholders	✓	✓	(<i>See 12 CFR Parts 337.3 and 349.3</i>)
<i>parts</i>	Subpart B – Reports of Indebtedness of Executive Officers and Principal Shareholders of Insured Nonmember Banks		✓	(<i>See 12 CFR Parts 337.3 and 349.3</i>)
337.3	Limits on Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Insured Nonmember Banks			✓
349.3	Reports by Executive Officers and Principal Shareholders			✓
563.43	Loans by Savings Associations to Their Executive Officers, Directors, and Principal Shareholders			✓

Table 2

For engagements involving management assertions about compliance by:

Dividend restrictions	National banks	State member banks	State nonmember banks	Savings associations
Read the following parts and/or sections of Title 12 of the United States Code:				
56 Prohibition of Withdrawal of Capital and Unearned Dividends	✓	✓		
60 Dividends and Surplus Funds	✓	✓		
1467a(f) Declaration of Dividends				✓
1831o Prompt Corrective Action-- Dividend Restrictions	✓	✓	✓	✓
Read the following parts and/or sections of Title 12 of the Code of Federal Regulations:				
5.61 Payment of dividends; capital limitation	✓			
5.62 Payment of dividends; earnings limitation	✓			
6.6 Prompt Corrective Action- Dividend Restrictions	✓			
7.6120 Dividends Payable in Property Other Than Cash		✓		
208.19 Payments of Dividends			✓	
208.35 Prompt Corrective Action				✓
325.105 Prompt Corrective Action				✓
563.134 Capital Distributions				✓
565 Prompt Corrective Action				✓

TABLE 24.1 LAW AND REGULATION REFERENCES		
Law/Regulation Cite	Reference	Responsible Agency
12 USC 363 ¹	FDIC Improvement Act	FDIC
12 USC 371c; Section 23-A	Transactions with Affiliates Federal Reserve Act, Section 23-A	FRB, OCC
12 USC 371c-1; Section 23-B	Restrictions on Transactions with Affiliates Federal Reserve Act, Section 23-B	FRB, OCC
12 USC 375	Purchases from Directors and Sales to Directors	
12 USC 1811 et seq ¹	Financial Institution Examination Reform, Recovery, and Enforcement Act of 1989	
12 USC 1820(d)	Examination Frequency	
12 USC 1861 - 1867 ¹	Bank Service Corporation Act	
12 USC 1972	Tying Arrangement for Correspondent Accounts	
15 USC 78(m)(b)	Foreign Corrupt Practices Act	
15 USC 271, 272, 278g-3 40 USC 758,759	Computer Security Act of 1987	
18 USC 1030	Computer Fraud and Abuse Act of 1986	
18 USC 1367, 2232, 2510 et seq, 2701 et seq, 3117, 3121	Electronic Communications Privacy Act of 1986	
18 USC 2510 et seq	Wire Interception and Interception of Oral Communications Act of 1968	
31 USC 5314	Foreign Financial Agency Recordkeeping (Reports of Currency and Foreign Transactions)	
12 CFR 7.1019	Electronic Products and Services	OCC
12 CFR 210	Collection of Checks and other Items by Federal Reserve Banks and Funds Transfer Through Fedwire Federal Reserve - Regulation J	FRB
12 CFR 225.22 ¹	Bank Holding Company Act	FRB
31 CFR 103.33	Bank Secrecy Act - Financial Recordkeeping (Reports of Currency and Foreign Transactions)	FINCEN ²

¹ These law cites are detailed more fully in Laws and Regulations (Chapter 24) of the Handbook.

² Financial Crimes Enforcement Network

TABLE OF CONTENTS

Number	Date	Subject
SP-1	9/91 (Rev.)	Interagency EDP Examination, Scheduling, and Report Distribution Policy Statement <i>Cross references:</i> FRB-SR-91-21 (10-11-91) OCC-EC-261 (1-24-92)
SP-2	10/78	Uniform Interagency Rating System for Data Processing Operations <i>Cross references:</i> FDIC-PR-104-78 (10-18-78)
SP-3	1/88	Joint Interagency Issuance on End-User Computing Risks <i>Cross references:</i> FDIC-BL-2-87 (1-25-88) OCC-BC-226 (1-25-88) FRB-SR 88-2 (1-21-88) OTS-TB-29 (3-22-88) NCUA-CUL-109 (9-1-89)
SP-4	11/88	Supervisory Policy on Large-scale Integrated Financial Software Systems (LSIS) <i>Cross references:</i> FDIC-BL-35-88 (12-5-88) OCC-AL-88-7 (11-21-88) FRB-SR-88-33 (11-30-88) OTS-TB-11 (12-9-88) NCUA-CUL-109 (9-1-89)
SP-5	7/89	Interagency Policy on Contingency Planning For Financial Institutions <i>Cross references:</i> FDIC-BL-22-88 (7-14-89) OCC-BC-177(Rev.)(7-12-89) FRB-SR-89-16 (8-1-89) OTS-TB-30 (7-19-89) NCUA-CUL-109 (9-1-89)
SP-6	1/90	Interagency Statement on EDP Service Contracts <i>Cross references:</i> FDIC-FIL-17-90 (3-5-90) OCC-BC-260 (7-14-92) FRB-SR-90-5 (1-24-90) OTS-TB-44 (2-7-90) NCUA-CUL-122 (2-91)
SP-7	3/90	Interagency Policy on Strategic Information Systems Planning for Financial Institutions <i>Cross references:</i> NCUA-CUL-122 (2-91)
SP-8	9/91	Interagency Document on EDP Risks in Mergers and Acquisitions
SP-9	4/93	Interagency Statement on EFT Switches and Network Services <i>Cross references:</i>

		OCC-BC-271 (5-25-93) FDIC-FIL-30-93 (4-29-93)	OTS-TB 59 (5-19-93)
SP-10	12/93	Interagency Document on Control and Security Risks in Electronic Imaging Systems	
		<i>Cross references:</i>	
		FRB-SR-94-2 (1-13-94) FDIC-FIL-13-94 (2-25-94)	OCC-94-8 (1-27-94)
SP-11	01/95	Enhanced Supervision Program (ESP) for Multidistrict Data Processing Servicers (MDPS)	
		<i>Cross references:</i> None	



Federal Financial Institutions Examination Council

SP-1
September 1991 Revised

Subject: Interagency EDP Examination, Scheduling And Distribution Policy

Purpose

This policy provides for joint examinations of data centers providing services to insured institutions supervised by more than one federal regulatory agency. It is expected to eliminate the need for separate examinations of data processors by more than one federal financial institution regulator and to result in more efficient use of examiner resources. This policy supersedes the previously issued interagency EDP examination policy, including the Multiregional Data Processing Servicers policy.

I. Examination Responsibility

Examination responsibility is determined based on the class/type of servicer as well as the class/type of insured financial institution(s) being serviced.

A. Insured Institutions

Data centers operated by an insured financial institution or its subsidiary will be examined by the federal regulatory agency responsible for the institution.

B. Financial Institution Holding Companies

Data centers operated by a holding company or its affiliate which service only one class of insured financial institution will be examined by the federal regulatory agency responsible for that class of institution.

Data centers operated by a holding company or its affiliate which service more than one class of insured financial institution will be examined jointly, or on a rotated basis, as agreed to by the federal regulatory agencies responsible for that class of institution.

Data centers operated by a holding company which controls only one insured financial institution, or its affiliate, will be examined by the federal regulatory agency responsible for the institution.

C. Independent Data Centers

Responsibility for the examination of independent data centers will be based on the class of insured financial institution being serviced. If more than one class of insured institution is serviced, the examination will be conducted jointly, or on a rotated basis, as

agreed to by the federal regulatory agencies responsible for that class of institution.

D. *Financial Institution Service Corporation*

Responsibility for the examination of service corporations will be based on the class of insured financial institution being serviced.

E. *Multiregional Data Processing Servicers (MDPS)*

MDPS examinations are to be conducted on a joint basis by the federal agencies having responsibility for the class of institution serviced. MDPS examinations will be administered by the FFIEC EDP Subcommittee of the Task Force on Supervision in Washington, D.C. The EDP subcommittee will determine the data centers subject to examination under the MDPS program. Generally, an organization will be considered for examination under the MDPS program provided: the organization processes major applications for a large number of insured financial institutions, thereby posing a high degree of systemic risk; or the organization processes work from a number of data centers located in diverse geographic regions.

No federal regulatory agency is precluded from conducting an independent examination of any data center that is providing data processing services to an insured financial institution for which the agency is responsible or where an agency has regulatory responsibility for holding company data centers.

II. Scheduling

Scheduling of joint/rotated EDP examinations and issuance of the EDP Report of Examination will be handled at the regional/district level. However, the examination of data centers under the MDPS program will be administered at the national level. A list of regions and contact personnel will be forwarded under separate cover and will be revised as appropriate.

A. *Joint and Rotated Examinations*

Regional/district representatives should meet annually (as early in the scheduling cycle as possible, but not later than December 1) to arrange for upcoming examinations and ensure that all data centers are examined in accordance with existing agency guidelines. As regional/district boundaries vary, it may be necessary for an agency to send representatives from more than one regional/district office to attend the scheduling meeting. Conversely, a representative may be required to attend more than one meeting. State agencies interested in participating in joint examinations may be invited to these meetings as deemed appropriate.

The meeting should identify all data centers, except for MDPS. Examinations of these data centers are to be conducted jointly and examination schedules agreed upon by participating agencies. If an agency cannot complete its schedule as agreed, it shall promptly notify the appropriate agencies so that alternative arrangements can be made.

When joint examinations cannot be scheduled, one agency will be designated to perform the examination on behalf of all concerned agencies. In these situations, examination responsibilities will be rotated for two-year periods. However, when the data center's overall condition is determined to be less than satisfactory, subsequent examinations should be conducted on a joint basis until the data center's overall condition is satisfactory as defined in the EDP Examination Handbook policy statement SP-2:

Uniform Interagency Rating System For Data Processing Operations.

The regional examination schedule should establish: the data centers to be examined; the date, time and agency responsible for any rotated or joint examinations; and the agency responsible for authoring and processing the examination report.

B. *Multiregional Data Processing Services*

Scheduling of MDPS examinations will be the responsibility of the FFIEC EDP Subcommittee of the Task Force on Supervision. By September 30 of each year, the EDP Subcommittee will prepare and publish an annual schedule for MDPS examinations designating the data center, the date of examination and the lead agency. This schedule will be distributed by the EDP Subcommittee agency representatives to their regional/district offices as soon as practical. An agency will be in charge of no more than two consecutive MDPS examinations.

Institutions with a composite rating of 1 or 2 will be subject to a full examination on a 24 month examination cycle, 3 rated institutions should be examined at an 18 month cycle and those institutions rated 4 or 5 at a 12 month cycle. The ongoing condition of MDPS should be monitored between examinations through periodic visitations and progress reports, as appropriate.

The lead agency is responsible for conducting a pre-examination review to determine: the scope of the examination, resource requirements, schedule of events and procedures to be followed during the course of the examination. At minimum this pre-examination report should provide details on the organization's: corporate history, corporate and organizational structure, scope of the upcoming examination, data centers included in the examination and examiner requirements. The pre-examination report should be forwarded to the Washington, D.C. office of the lead agency at least 60 days prior to the commencement of the MDPS examination.

Examinations of individual data centers or processing sites may commence prior to the start of the headquarters examination if more than one facility is involved. However, these time frames must be approved by the lead agency.

III. Report Preparation

A. *Joint Examinations*

Responsibilities will be divided among the EDP examiners assigned to the examination. When preparing joint examination reports, the participating agencies are required to reach agreement on the report comments. In rare instances when agreement cannot be reached at the regional level, the differences should be appealed to the Washington office of the participating agencies for final resolution.

The processing of the final Report of Examination (FFIEC 007) is the responsibility of the authoring agency. All changes made to the joint report in the course of its processing should be approved by the regional staffs of the agencies participating in the examination.

B. *MDPS Examinations*

Only one consolidated Report of Examination will be prepared by the lead agency. The

objective is to give the overall view of the organization, not each individual data center comprising the Multiregional Data Processing Servicer. However, the relative strength of each facility should be evaluated. In some instances it may be necessary to issue a specific data center report, although such action would be taken at the discretion of the EIC and the lead agency's Washington office.

IV. Report Distribution Policies and Procedures

A. *Joint Examinations*

The lead agency is responsible for providing each affected federal and state banking agency with a copy of the completed report, including the Administrative Section. (A complete list of all serviced financial institutions, by charter, should be included in this section as well.) Each agency is responsible for reproducing the report

comments and distributing them to serviced institutions in accordance with the provisions below. A transmittal letter will be used to advise each recipient that the comments are for their internal use only, are not to be construed to satisfy audit requirements and remain the confidential property of the lead agency. A written receipt will be obtained from each recipient.

In all instances, examination reports should be distributed to the board of directors of the examined data center. Where the data center is a subsidiary of a holding company, the report should be forwarded to the board of directors of the data center, where applicable, or otherwise senior management of the data center and to the board of directors of the holding company. In the case of a service corporation, a copy should be forwarded to the corporation's board of directors as well as to the board of directors of each financial institution owning stock in the corporation.

Independent Service Bureau reports should be directed to the board of directors or senior management of the servicer. If the independent service bureau is a branch of a multi-branch servicing organization, an additional copy should be forwarded to the board of directors at the corporate headquarters.

Distribution of examination reports to serviced institutions for joint examinations will be at the discretion of the federal regulatory agency responsible for regulating the institution serviced, except for data centers rated composite 4 or 5, which must be distributed to all insured serviced institutions. Where an examination report is to be distributed by a participating agency, the lead agency must be so notified prior to transmitting the examination report. When an examination report is requested by a serviced financial institution, only the examiner's conclusions, recommendations and comments are to be transmitted to the serviced institutions. Matters of a proprietary or competitive nature relating to the servicer will be excluded from the report comments prepared for distribution to serviced institutions, but will be contained in the report provided to the servicer and the other federal agencies. In cases where the servicer fails to respond to corrective action requests, it may be necessary to report the uncorrected deficiencies to the serviced institutions. In these situations, the regulatory agencies of all serviced institutions must be in agreement regarding the need for this course of action and must meet with the servicer to convey this intent.

The FFIEC interagency procedures do not affect existing distribution agreements with state agencies. However, no state agency shall distribute examination reports to any serviced institution without the express consent of the lead agency. Only the agency

conducting the examination will provide nonparticipating state authorities copies of the report. In the case of joint examinations, participation by state agencies and report distribution to those state agencies will be decided on an individual basis at the district/regional level by the participating federal agencies.

B. *MDPS Examinations*

The consolidated report of examination should be sent to the Washington office of the lead agency and to the board of directors of the data servicer. The lead agency's Washington office is to provide a copy of the report to the other FFIEC EDP Subcommittee members for distribution to the respective agency regional/district offices. The agency in charge is responsible for sending a copy of the report to the appropriate state supervisory agencies. Excluding the provisions noted above, distribution of MDPS reports should otherwise be in accordance with the provisions governing the distribution of joint interagency examinations.



Federal Financial Institutions Examination Council

**SP-2
October 1978**

Subject: Uniform Interagency Rating System For Data Processing Operations

The rating system for data processing operations is similar to the "Uniform Interagency Bank Rating System," which is based upon an evaluation of the overall performance of a bank. The EDP rating system is based upon an evaluation of four critical functions of a data processing operation: audit, management, systems development and programming, and computer operations. Each data center will be assigned a summary or composite rating based upon the separate performance ratings assigned these four functions.

Each performance rating and the composite rating are based on a scale of 1 through 5, with 1 representing the highest and 5 the lowest rating. Each function must be evaluated in order to determine its performance rating. To arrive at composite rating, due consideration must be given to the interrelationships and relative importance of the four functions. Occasionally there will be factors that are not reflected in any specific performance rating but are important to the data center's overall condition and should be reflected in the composite rating.

A general description of each performance rating is as follows:

Rating No. 1 – Strong performance.

Performance that is significantly higher than average.

Rating No. 2 – Satisfactory performance.

Performance that is average or slightly above and which adequately provides for the safe and sound operation of the data center.

Rating No. 3 – Fair performance.

Performance that is flawed to some degree and is considered to be of below average quality.

Rating No. 4 – Unsatisfactory performance.

Performance that is significantly below average and, if left unchecked, might evolve into weaknesses or conditions which could threaten the integrity of the records processed and the viability of the institution or data center.

Rating No. 5 – Hazardous performance

Performance that is critically deficient and in need of immediate remedial attention. Such performance threatens the integrity of the records being processed and the viability of the institution or data center.

A general description of each composite rating is as follows:

- Composite 1*** Data centers in this group are sound in almost every respect. If deficiencies are noted, they are of a minor nature and can be handled in a routine manner without further supervisory involvement.
- Composite 2*** Data centers in this group are also fundamentally sound but may reflect modest weaknesses. Deficiencies are generally corrected in the normal course of business. Therefore, the need for supervisory response is usually limited.
- Composite 3*** Data centers in this group are experiencing a combination of adverse factors which require prompt corrective action. Problems are well defined and require more than ordinary supervisory concern and monitoring. The overall strength of management and supporting staff and the financial capacity of the data center are such as to make operation failure only a remote possibility.
- Composite 4*** Data centers in this group are operating under unacceptable conditions which could impair future viability. A high potential for operational and/or financial failure is present. Although a high potential for failure is present, weaknesses are not so severe as to threaten the immediate failure of the data center. Immediate affirmative action and supervision by the regulator are necessary.
- Composite 5*** Data centers in this group exhibit a combination of weaknesses and adverse trends which are pronounced to a point where the ultimate continuation of the operation is in serious question. Immediate affirmative action and continuous supervision, as required by the regulator, are necessary.

The four functional areas which are rated and the areas of consideration under each one are:

AUDIT

Audit is rated (1 through 5) with respect to:

- A. Organization
 - Independence
 - Board of directors' support
 - Resources allocated
 - Management and staff succession
- B. Staff Qualifications Training
- C. Quality of Audits Scope
 - Frequency
 - Standards and procedures
 - adequacy
 - compliance
 - Follow up and correction of exceptions
 - Working papers and documentation
 - completeness
 - security
 - Audit software
 - use
 - effectiveness
 - documentation
 - Audit reports

respect to:

- A. Organization
 - Resources allocated
 - Leadership
 - Administrative abilities
 - Qualifications
 - Delegation of responsibilities
 - Support
 - Management succession
- B. Correction of Deficiencies
- C. Laws and Regulations
 - Awareness
 - Compliance
 - Contracts
- D. Planning
 - Risk analysis
 - User involvement
 - Senior management involvement
 - Budget
- E. Standards and Procedures
 - Development
 - Enforcement
- F. Internal Controls
 - Development
 - Enforcement
- G. Physical Security
 - Development
 - Enforcement
- H. Financial Condition

SYSTEMS DEVELOPMENT AND PROGRAMMING

Systems and programming is rated (1 through 5) with respect to:

MANAGEMENT

Management is rated (1 through 5) with

-
- | | |
|---|--|
| <p>A. Organization
 Separation of duties
 Resources allocated
 Management and staff succession</p> <p>B. Staff
 Qualifications
 Training</p> <p>C. Standards and Procedures
 Adequacy
 Compliance
 User liaison</p> <p>D. Documentation
 Completeness
 Organization
 Storage and security</p> <p>E. Internal Controls
 Modification and change procedures
 authorization
 – documentation
 – implementation
 Program library maintenance
 Systems development</p> <p>F. Physical Security
 Documentation
 Software
 On-line systems</p> | <p>Management and staffing
 succession</p> <p>B. Staff
 Qualifications
 Training</p> <p>C. Standards and Procedures
 Adequacy
 Compliance
 User liaison</p> <p>D. Operations
 Data entry control
 Processing controls
 Output distribution controls
 Physical security
 Emergency plans
 User communication</p> |
|---|--|

COMPUTER OPERATIONS

Computer operation is rated (1 through 5)
 with respect to:

- A. Organization
 Separation of duties
 Resources allocated



Federal Financial Institutions Examination Council

**SP-3
January 1988**

Subject: Joint Interagency Issuance on End-User Computing Risks

**To: Chief Executive Officers of all Federally Supervised Financial Institutions,
Senior Management of each FFIEC Agency, and all Examining Personnel**

Purpose:

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

Background:

In recent years, microcomputers, or "personal computers", 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.

Concerns:

Technology, using microcomputers as end-user computing devices, has taken data processing out of the centralized control environment and introduced the computer related risks in new areas of the banks. 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 has 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.

Bank management 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. Such a policy should address areas such as:

- management controls,
- data security,
- documentation,
- data/file storage and backup,
- 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 issuance provides more detail regarding the risks and suggested controls for end-user computing and other computer related activities. Additional control recommendations can be referenced in the FFIEC EDP Examination Handbook.

Policy:

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, has 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 the examiners during the regular supervisory reviews of the institution.

SP-3 - APPENDIX

Risks And Controls In End-User Computing

Microcomputers, in the end-user computing operations, are being used basically for three purposes:

- 1) as word processors,
- 2) as communications terminals with other computers (to transmit or receive information in their databases), and
- 3) as stand-alone computer processors.

These three functions require different control objectives, based on the risks associated with the activity. Each function requires certain operational type controls such as physical security, logical security, and file backup. However, the more pronounced risks involve those operations using microcomputers as stand-alone processors.

While word processing and terminal communications also require strong controls, programming support for the operating software and applications systems generally remain centralized or is a vendor responsibility. In end-user computing, the user is often engaged in program development, in addition to information processing. This may involve the creation of programmed software from an original design or building customized routines from specialized vendor software. Regardless, the control techniques for the programming, its testing, and its documentation are necessary to ensure the integrity of the software and the production of accurate data.

In addition to the programming activity, the end-user environment supports computer processing, which may be totally separate from centralized controls. Information may be downloaded from the main databases and reprocessed by the end-user. Data may also be originated for processing in this structure. Regardless of the source, the resulting information is relied upon by management for decisions impacting corporate strategies and customer relationships. The integrity of the data becomes no less important than had the data been produced through more sophisticated computer processes. Likewise, the need for control at the micro level remains equally important.

Impacts

The failure to properly implement a uniform set of controls on the end-users of microcomputers, consistent with those controls required in a mainframe data center, can create two broad categories of risks:

- 1) the corruption or loss of data and/or program software, and
- 2) impediments to the efficient operation and management of the bank.

The quality of data is paramount to the successful management of any institution. Should the data, or the systems which produce that data, be corrupted, whether intentionally or unintentionally, financial loss is highly probable. Data corruption could result from three basic causes: error, fraud, or system malfunction.

In addition to accuracy, management requires the timely availability of data. Inefficiencies,

caused by poor operational controls, can further impede the production of information and result in financial loss. Regardless of the source, poor quality information and operations can adversely impact the bank in a number of ways:

- *Management Error* – Inaccurate or incomplete data can adversely influence bank management decisions. Delays in information availability can also adversely impact corporate strategies.
- *Inadvertent Disclosure* – Human error, fraud, or system malfunction may result in proprietary bank data, customer data, or program software being disclosed to unauthorized persons.
- *Competitive Disadvantage* – Problems in the production of accurate and timely information can place the bank at a competitive disadvantage. Delivery of services, customer confidence, and management decisions could be impaired.
- *Legal Problems* – Errors in the production of data or wrongful disclosure of data may result in legal actions against the bank by its customers, consumer groups, competitors, and regulators.
- *Regulatory Problem* – Failure to produce timely and accurate data can cause the bank to be in violation of regulatory requirements, subjecting the bank to regulatory penalties.
- *Monetary losses* to the bank can arise from deliberate manipulation of the data (fraud), missing or erroneous data (leading to costly incorrect decisions), or various inefficiencies in the operation of the system.

Controls

There are basic controls which should be present in any level of computer operations. These controls should already be present at the centralized data center. The evolution of microcomputer-based systems has not eliminated the need for these basic controls, but has shifted the focus of control to the end-user level.

Some of these basic control standards that need to be implemented in microcomputer-based systems are:

Policies and Procedures

Control requirements for microcomputer use need to be addressed by management in its internal policies and procedures. Policies and procedures should be in writing and should define what steps are to be taken to protect the bank's microcomputer systems. Management should also designate responsibility within the bank to monitor microcomputer system acquisition and use. The purpose of this function should be to help prevent redundant uses of microcomputer systems and to ensure that there is the required degree of compatibility among hardware and software systems in use throughout the bank.

Program Development and Testing

Before a new system is developed or purchased, the user should have a clear understanding of the specific needs being addressed by the proposed new system. Alternatives should be reviewed by the user and analyst to ensure that the best solution is selected. Development should be done with the aim of producing a system that is easily modified and maintained by someone other than the original developer. Finally, the completed system should be subject to rigorous testing to provide

assurance that the results produced are valid and reliable.

Program Changes

Just as with larger systems, microcomputer systems must be adapted to meet changing requirements and circumstances. Modified programs should be subject to many of the same controls as newly-developed systems. Most important among these is the requirement that there be thorough testing of the modified system. In addition, accurate records should be maintained describing the change, the reasons for the change, and the person responsible for making the change.

Documentation

Documentation is a potential problem in microcomputer-based systems. There is a tendency for these systems to be highly personalized, with one person fully responsible for the development, testing, implementation, and operation of a set of programs. The successful use of a microcomputer-based system and the production of specialized data may depend on the continued presence of this one person. An adequate level of documentation helps to prevent an over reliance on the knowledge of this one person. This is particularly needed should revisions to programs be required. Documentation standards should define acceptable levels of program, operating, and user documentation. In addition, there should be an enforcement mechanism to guarantee compliance with standards.

Data Editing

The development or purchase of microcomputer systems should be done with adequate attention given to the need for data editing routines. These routines are important to help ensure that data entering the system is error-free and not likely to result in erroneous output. This control is important whether the data is being manually entered into the microcomputer or electronically transferred or "downloaded" from another system. In the case of data being "uploaded" to a mainframe, additional controls may be required at that level to guarantee the integrity of the data being transferred.

Input/Output Controls

Microcomputer systems that are used for the processing of information with a direct monetary impact on the bank or its customers may require that additional data controls be established. At a minimum, these controls may include the requirement that there be a segregation of duties between the input of information and the review of that information in processed form. This control may be extended to require that a formal reconciliation be done by the reviewer of the processed information. In more sensitive situations with a significant dollar impact, there may be a requirement that certain functions be performed under dual control. The need for these types of input and output controls should be established during the early stages of program development. These special requirements need to be described in detail in the program documentation package.

Physical Access Restrictions

The location of microcomputer systems outside of a physically-secure data center can permit unauthorized access to programs and data files used on these systems. The use of physical access restrictions complements the logical access restrictions discussed below. Basic steps would include the secure storage of diskettes or other magnetic media containing the programs and data for a particular system. In addition, since documentation on what a system does and how it is being used can provide important information that can be used to compromise system security,

this information should also be secured. Finally, there should be adequate restrictions over physical access to the hardware itself, so that it is protected from unauthorized use, vandalism, and theft.

Logical Access Restrictions

Just as in larger application systems, the need exists to identify those individuals who will be permitted access to the microcomputer system's capabilities. In addition, there may be the need to differentiate between functions allowed for certain individuals, ranging from an inquiry capability for many persons to an override and correction capability for a few supervisory personnel. Normally, these restrictions will be in the form of password controls. Standard password-related control procedures, such as frequent changes and reporting of exception conditions need to be established to provide for effective access restrictions.

Backup and Contingency Planning

For each operational system, adequate plans should be made and precautions taken to ensure that users can adequately recover from damage to the hardware, software, and data. For some systems, an inability to process during recovery may mean that work can be held for later processing. For other systems, a manual backup may be appropriate. For some time critical, highly automated systems, arrangements may have to be made for data reconstruction or for processing on other hardware. At a minimum, for all systems, there should be secure and remote backup storage of data files and programs. Beyond this, the backup and contingency requirements for individual systems may differ and need to be addressed separately.

Audit

The audit area should serve as an independent control reviewing microcomputer use throughout the bank. Audit involvement in microcomputer systems may begin at a general level with a review for compliance with the internal policies and procedures discussed above and may extend to detailed testing in particular areas such as the use of logical access controls. Audit procedures and workprograms should be expanded to provide for adequate coverage of microcomputer systems. Responsibility for microcomputer auditing should be clearly assigned and plans for microcomputer audits should be built into the audit schedule.

It should be recognized that this list of controls is not all inclusive of methods to manage risk. Each computer operation. Whether centralized or end-user, possesses different characteristics and possibly some specialized risks. Control practices must be sufficient to minimize such risks. These recommended control features are considered fundamental to sound information processing.



Federal Financial Institutions Examination Council

**S
P
-
4**

November 1988

**Subject: Supervisory Policy On Large Scale Integrated Financial
Software Systems (LSIS)**

**To: Chief Executive Officers of all Federally Supervised Financial Institutions,
Senior Management of each FFIEC Agency, and all Examining Personnel**

Financial institutions have experienced significant problems in attempts to introduce LSIS systems.

- After 2-1/2 years in development, one financial institution abandoned \$20 million large scale integrated system!
- After 5 years in development, a major software vendor abandoned \$100 million integrated system once described as the perfect software system for regional banks!

Purpose

Financial institution executives and directors should be aware of and concerned about the potential problems with LSIS. The purpose of this paper is to alert financial institutions to the risks associated with these systems and to identify management's responsibilities when entering into an LSIS project.

Background

"An integrated software system is one in which programs for different applications – loans, deposits, retail, and wholesale – that normally are designed and operated as stand alone programs are built from the start as related parts of a whole. They share a common language, operating system, and other technical details so that they can be made to `talk' to each other with relative ease. More importantly, they function as one unit so that the sum of the parts is greater than the whole." ¹

Financial institutions are adopting LSIS in order to meet competitive pressures, increase timeliness of information, foster operational efficiency, and ease introduction of new products. A commitment to LSIS sets the course of an institution's technology, management information system, and delivery systems for several years. Successful implementation of LSIS requires careful planning by both senior management and the board of directors.

¹ Christopher K. Heaney, "Who are these guys anyway?" ABA Banking Journal, May 1986, pp. 84-85 and development process. When these projects experienced lengthy delays, the financial institutions not only suffered large monetary losses but also delays in product development and a loss in their competitive positions.

Ineffective planning caused several financial institutions and software companies to spend millions of dollars and years of conversion and implementation time on LSIS, only to implement a portion of the system or in some cases abandon the project altogether. In many instances, the software vendors depended upon substantial ongoing investment by the financial institutions to fund the vendor's research

Concerns

Financial institutions have underestimated the cost, time and personnel resources required for the successful installation of LSIS. Therefore, time and cost targets should be established at the beginning of the project and closely reviewed by senior management on an ongoing basis.

In certain cases LSIS projects were abandoned because of the financial instability of software vendors. To prevent these situations from recurring, the financial condition and viability of each prospective vendor must be considered when evaluating systems.

Data backup and recovery measures for integrated systems are often more costly than those required for single application systems. In certain situations, the data base may require simultaneous backup. The additional costs for backup and recovery must be evaluated when determining the feasibility of LSIS.

If the system provides for instantaneous update of information – in other words, the user has direct access to the data – existing security systems may not be adequate. Thus, data security features must be evaluated to ensure that sufficient controls exist for LSIS.

Seemingly simple program changes can have unpredictable results in a mixed-application system. Thus, system development life cycle methodologies, which identify the sequence of activities required in the systems development process and throughout the useful life of the software, may need to be modified.

There is an increased possibility of unwarranted data manipulation and at the same time, there is less of an audit trail in an LSIS environment. Therefore, EDP audit coverage should be reviewed at the onset to determine whether specialized audit techniques are needed.

Board of Directors and Senior Management Responsibilities

The decision to acquire or develop in-house large-scale integrated software should be preceded by a strong and independent management planning process. This should include a thorough examination of existing software performance. Also, a detailed analysis of the system's capability to meet the institution's strategic business plans is essential.

The complexity of the software and its impact on the entire organization require a commitment from top management for the project to be successful. Responsibility for the conversion should be clearly identified and established at the senior management level.

Senior management should regularly review the project's status. This improves control over the complex process of implementation and ensures completion within established time and cost targets. It is particularly important that the board continue its oversight responsibilities after implementation.

The attached pages discuss the impact and responsibilities associated with LSIS.

SP-4 - APPENDIX

Large-scale Integrated Financial Software Systems

Definition and Scope

Large-Scale Integrated Systems (LSIS) are sophisticated software products which provide interconnections and facilitate the exchange of information between applications and functions. The integration architecture may be horizontal, tying together applications, such as deposits, loans, and general ledger. Alternatively, the architecture may be vertical, tying together functions, as in teller transactions being linked immediately to all operating departments. These systems are designed so that each application no longer exists individually but operates as part of a unified system. They often employ data base management technology, which increases the complexity of the system. LSIS processing may employ combinations of batch, online, or memo methods. A variety of LSIS are being marketed and others are in various stages of development.

Small-to-medium size financial software systems whose applications simply interfaced through a Central or Customer Information File (CIF) have been operating for many years. Many of these systems have been successfully installed and have operated properly for a considerable period. These systems are not included in the scope of this issue paper, although they are sometimes described as "integrated systems."

Advantages of Large-Scale Integrated Systems

- Provide tools to increase product line and customer relationships, ultimately increasing fee income on deposit and loan services.
- Enable financial institutions to meet competition generated from forces outside the banking industry.
- Lower the unit processing costs through standardization of operating techniques.
- Eliminate redundancy in data files.
- Provide information at more points throughout the institution, enabling faster and more accurate management decisions.

Disadvantages of LSIS

- The complexity and size of large-scale integrated systems can lead to underestimation of the time and resources needed for successful installation of these systems.
- The magnitude of the installation effort requires more comprehensive management techniques and project control.
- The financial instability of the software vendor may require the institution to furnish unplanned additional financial support to maintain contemplated service levels.
- The failure to properly install the software can lead to significant losses to the institution, in terms of time and resources expended, and a decline in competitive position.

Internal Control Related Concerns

- **Data Security:** Data security should be addressed prior to the installation of such a system. Existing data security systems may not be adequate for a complex integrated

system, particularly one using on-line real-time processing. Each individual function should be controlled, e.g. access controls, file maintenance, inquiry, and new accounts.

- EDP Auditing: A greater chance of unwarranted data manipulation and a diminished audit trail exists. Therefore, institutions should recognize the need for expanded EDP audits of this technology, especially in an on-line real-time environment.
 - Absence of Acceptable Audit Trails – When a system allows the automatic generation of a transaction prompted by a prior transaction, controls must be designed within the system to ensure satisfactory audit trails. This is especially critical considering that a single transaction may generate several other transactions.
 - Accountability for all transactions must be maintained through audit trails. Otherwise, system integrity deficiencies will jeopardize the software system's ability to provide a consistent product, as well as compromise internal controls.
 - Absence of Comprehensive Audit Software – Existing generalized audit software may not be readily adaptable for use with large-scale integrated systems, and may not be sufficiently sophisticated to follow an audit trail of all transactions generated by the system. Provision for audit software should be made at the time of system acquisition.
- Disaster Recovery Planning: Integrated systems have unique features which will require a thorough consideration of contingency requirements in the initial feasibility study. The complexity of the integration, horizontally, vertically, or both, may determine that current industry standards for the backup of hardware, software, data and communications are no longer applicable. A determination should be made how the institution, as a whole, will recover and how recovery will be addressed along functional lines. Subsequently, required testing may pose cost, logistical or other problems which will have to be resolved to ensure a viable disaster recovery plan.
- Changes in System Development Life Cycle (SDLC) Methodology: There are several significant control issues regarding the use of traditional SDLC methods with large-scale integrated systems. Current system development techniques may not permit the timely development and implementation of a complex system. SDLC techniques may need to be revamped to provide for increased flexibility. However, control and management methods may vary according to the complexity of the system under development.

Minimum SDLC standards should ensure that project development is sufficiently controlled to provide for the integrity of the system. Testing of various stages within large scale integrated systems may require innovative techniques.

Management should carefully consider the cost of the extensive user involvement in the system development stage. User involvement is necessary to ensure the successful implementation of a large scale integrated system.

Management must provide more comprehensive employee training since the adoption of a LSIS will affect all departments.

SDLC standards need to be flexible, while still providing for the maintenance of system integrity during development to ensure that a system of internal control is maintained.



Federal Financial Institutions Examination Council

**SP-5
July 1989**

Subject: Interagency Policy On Contingency Planning For Financial Institutions

**To: Chief Executive Officers of all Federally Supervised Financial Institutions,
Senior Management of each FFIEC Agency, and all Examining Personnel**

Purpose

The purpose of this policy statement is to alert the Board of Directors and management of each financial institution to the need for contingency planning for their institution. This includes both institutions that provide their own information processing service and those that receive processing from service companies. The policy statement also addresses issues that should be considered when developing a viable contingency plan.

Background

Contingency planning is the process of identifying risks from disruption of operations and services. The objectives are to:

- minimize disruptions of service to the institution and its customers,
- minimize financial loss, and,
- ensure a timely resumption of operations in the event of a disaster.

These strategies are the same for institutions with in-house data centers and those using service bureaus.

In recent years, information technology has expanded rapidly throughout the corporate structure of financial institutions. It includes operations such as central computer processing, distributed processing, end user computing, local area networking, and nationwide telecommunications. These operations often represent critical services to institutions and their customers. The loss or extended disruption of these business operations poses substantial risk of financial loss and could lead to the failure of an institution. As a result, contingency planning now requires an institution-wide emphasis, as opposed merely focusing on centralized computer operations.

Additionally, there are many service bureaus that provide information processing services to multiple financial institutions. The disruption of the processing capabilities of one of these service bureaus could impact a considerable number of institutions. Accordingly, contingency planning by financial institution servicers is equally important.

Concerns

Many financial institutions and service bureaus have not sufficiently addressed the risks associated with the loss or extended disruption of business operations. More specifically:

- Many contingency plans do not address all of the critical functions throughout the institution.
- Many service institutions have not established or coordinated contingency planning efforts with their service bureaus.
- Many service bureaus have not established contingency plans.
- Many contingency plans have not been adequately tested.

Policy

The board of directors and senior management of financial institutions are responsible for:

- Establishing policies, procedures and responsibilities for comprehensive contingency planning
- Reviewing and approving the institution's contingency plans annually, documenting such reviews in board minutes.

If the institution receives information processing from a service bureau, management also must:

- Evaluate the adequacy of contingency plans for its service bureau.
- Ensure that the institution's contingency plan is compatible with its service bureau's.

The appendix to this policy statement provides an example of a process that management may consider in developing contingency plans. It is a brief outline and is not all encompassing. Each financial institution needs to assess its own risks and develop strategies accordingly. This planning process needs to address each critical system and operation, whether performed on site, at a user location, or by another company.

SP-5 - APPENDIX

Contingency Planning Process

- I. Obtain commitment from senior management to develop the plan.
- II. Establish a management group to oversee development and implementation of the plan.
- III. Perform a risk assessment.

Consider possible threats such as:

- natural – fires, flood, earthquakes, ...
- technical – hardware/software failure, power disruption, communications interference, ...
- human – riots, strikes, disgruntled employee, ...

Assess impacts from loss of information and services:

- financial condition
- competitive position,
- customer confidence
- legal/regulatory requirements.

Analyze costs to minimize exposures.

- IV. Evaluate critical needs.
 - functional operations
 - key personnel
 - information
 - processing systems
 - documentation
 - vital records
 - policies/procedures
- V. Establish priorities for recovery based on critical needs.

- VI. Determine strategies to recover.
 - facilities
 - hardware
 - software
 - communications
 - data files
 - customer services
 - user operations
 - MIS
 - end-user systems
 - other processing operations.

- VII. Obtain written backup agreements/contracts.
 - facilities
 - hardware
 - software
 - vendors

-
- suppliers
 - disaster recovery services
 - reciprocal agreements

VIII. Organize and document a written plan.

Assign responsibilities.

- management
- personnel
- teams
- vendors

Document strategies and procedures to recover.

- procedures to execute the plan
- priorities for critical vs. non-critical functions
- site relocation (short-term)
- site restoration (long-term)
- required resources
 - human
 - financial
 - technical (hardware/software)
 - data
 - facilities
 - administrative
 - vendor support

IX. Establish criteria for testing and maintenance of plans.

Determine conditions and frequency for testing.

- batch systems
- on-line systems
- communications networks
- user operations
- end-user systems

Evaluate results of tests.

Establish procedures to revise and maintain the plan.

Provide training for personnel involved in the plan's execution.

X. Present the contingency plan to senior management and the Board for review and approval.

(Note: Additional guidelines in this area are available in Chapter 10 of the 1996 FFIEC IS Examination Handbook). Also, many materials on contingency/disaster recovery planning have been published by trade associations, accounting firms, and the disaster recovery industry. These can be valuable guides to comprehensive contingency planning.



Federal Financial Institutions Examination Council

**SP-6
January 1990**

Subject: Interagency Statement on EDP Service Contracts

**To: Chief Executive Officers of all Federally Supervised Financial Institutions,
Senior Management of each FFIEC Agency, and all Examining Personnel**

Purpose

This interagency statement alerts financial institutions to potential risks in contracting for EDP services and/or failing to properly account for certain contract provisions.

Issue

Some financial institutions are entering into EDP servicing contracts that contain provisions which may adversely affect the institution. Contract provisions may include extended terms (up to ten years), significant increases in costs after the first few years, and/or substantial cancellation penalties.

In addition, some service contracts improperly offer inducements that allow an institution to retain or increase capital by deferring losses on the disposition of assets or avoiding expense recognition for current charges. Institutions experiencing earnings and capital problems are particularly attracted to these inducements.

Examples of inducements include:

- The servicer purchasing assets (e.g., computer equipment or foreclosed real estate) at book value, which exceeds current market value;
- The servicer providing capital by purchasing stock from the institution;
- The servicer providing cash bonuses to the institution once the conversion process is complete; and
- The institution deferring expenses for conversion costs or processing fees under the terms of a lease or licensing contract.

These inducements offer a short-term benefit to the institution. However, the servicer usually recoups its costs by charging a premium for the data processing services it provides. These

excessive data processing fees adversely affect an institution's financial condition over the long-term. Furthermore, the institution's accounting for such inducements typically is inconsistent with generally accepted accounting principles (GAAP) and regulatory reporting requirements.

Title II, Section 225 of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 states:

An (FDIC) insured depository institution may not enter into a written or oral contract with any person to provide goods, products or services to or for the benefit of such depository institution if the performance of such contract would adversely affect the safety or soundness of the institution.

Accordingly, when negotiating contracts, an institution must ensure that the servicer can provide a level of service that meets the needs of the institution over the life of the contract. It is also the responsibility of the institution to ensure that contracts are accounted for in accordance with GAAP.

In summary, contracting for excessive servicing fees and/or failing to properly account for such transactions is considered an unsafe and unsound practice. Servicing agreements that include contract provisions or inducements similar to those discussed above should be closely reviewed by the institution. Institutions must ensure that accounting under such agreements reflects the "substance" of the transaction, not merely the "form."

Although this statement focuses on contracting for EDP services, these same issues may exist in contracts for other vital services.



Federal Financial Institutions Examination Council

**SP-7
March 1990**

Subject: Interagency Policy on Strategic Information Systems Planning for Financial Institutions

Purpose

This policy issuance alerts all financial institutions to the importance of strategic information systems planning and its role in overall corporate management and planning. It identifies management's responsibilities in preparing strategic plans for their information systems requirements.

Background

Information is a valuable corporate asset which is vital to the success of all financial institutions. The ability to remain competitive, introduce new products and services, and attain desired corporate goals often depends on the effective management of information systems technology.

Corporate level strategic planning is important in all financial institutions to effectively utilize available resources and achieve the long term goals and objectives of the organization. Strategic information systems planning is integral to the overall corporate strategic planning process and must support individual business strategies throughout the institution. The information systems strategic plan should address technology risks affecting all areas of operation, including contingency planning and disaster recovery, information security, systems and programming, computer operations, and end-user computing.

Effective strategic planning considers the impact of technology on the internal and external concerns of the institution. Internal issues are those where management has planning control. This includes profitability, delivery of new products and services, efficient and consistent operations, and corporate strategic planning. External issues are those over which management has no direct control, but must react to in a timely manner. These include technological advancements by competitors, regulatory requirements, and changing economic environments.

Strategic information systems planning is generally structured to address two primary objectives.

1. Build a technology strategy to assure that systems are:

- Cost effective in meeting business objectives;
- Timely (i.e. available when needed);
- Flexible (i.e. expandable/contractible);
- Efficient (i.e. competitive parity and competitive advantage); and

-
- Reliable (i.e. complete and accurate data).
2. Provide a system architecture integrating hardware, software, and telecommunications to assure:
- Proper collection and processing of information;
 - Availability of information, as required, at different locations; and
 - Proper distribution of applications.

Policy

Financial institutions should develop and implement a written strategic information systems plan commensurate with the complexity and sophistication of the institution. The plan should be integrated into overall corporate goals and should include in-house, end-user, and service bureau processing, as applicable. Successful implementation of a strategic information systems plan requires the board of directors of an institution to:

- Provide adequate oversight, including the review and approval, of business objectives and related information systems strategies;
- Ensure the ongoing development and implementation of the information systems plan;
- Ensure the technology strategy considers the size and complexity of the institution, the markets it pursues, and the nature of the products and services it offers; and
- Ensure the design of the organizational structure includes well defined delegations of authority commensurate with information systems technology.

The attached appendix provides additional guidance relating to strategic information systems planning.

SP-7 - APPENDIX

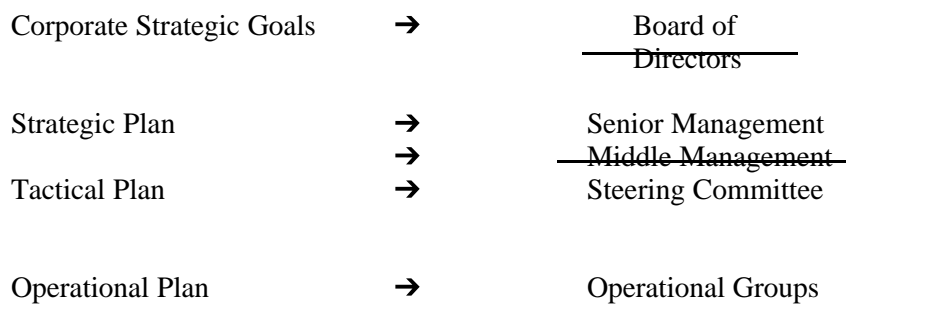
Board of Directors Oversight

The board of directors is responsible for reviewing and approving corporate strategies to ensure the continuance of successful operations. Oversight includes periodic review and approval of overall business objectives. This review should ensure coordination of the information systems plan with the overall corporate strategic plan. The monitoring process should reflect changes in current systems development. These changes should be reported in summary format in board and steering committee minutes.

Oversight activities include:

- Reviewing cost benefit analyses;
- Monitoring periodic performance/status reports;
- Ensuring that goals are consistent with overall corporate goals and safety and soundness;
- Implementing the plan through the effective utilization of financial resources, personnel skills and methodologies;
- Reviewing contingency/recovery policies on an annual basis; and
- Evaluating acquisition/merger conversion plans.

The following diagram and definitions illustrate the flow and structure of the planning hierarchy:



CORPORATE STRATEGIC GOALS

The board of directors establishes long term corporate goals and objectives for the financial institution. More specifically, the board determines the institution's current market position, methods needed to gain a competitive edge, and resources required to achieve the desired goals.

STRATEGIC PLAN

This plan defines the future direction and mission of the institution. It may be revised every two years and encompasses a time span of three to seven years. Its scope includes target markets, resources, technologies, and other appropriate criteria. Results show a framework and vision for

the institution's future direction. This plan is the backbone for supporting tactical plans.

TACTICAL PLAN

This is a program of action over a two-to five-year time period. It is updated annually and focuses more narrowly on the broad scope identified in the strategic plan. It results in a determination of specific activities, budgets, opportunities, and functional objectives.

OPERATIONAL PLANS

Often these plans list specific actions and milestones by month to achieve project plans, budgets, management by objective (MBO) agreements, and commitments. The plan life-cycle is generally for one year and can be subject to numerous updates and revisions.



Federal Financial Institutions Examination Council

**SP-8
September 1991**

Subject: Interagency Document on EDP Risks in Mergers & Acquisitions

To: Senior Management of each FFIEC Agency

Background

In recent years, mergers and acquisitions within the financial industry have increased significantly. With the changes in interstate banking laws many financial institutions have pursued mergers and acquisitions to enhance asset growth, gain market penetration, and to achieve a competitive advantage over rival institutions.

During the week of May 7, 1990 senior EDP examiners of the FFIEC member agencies participated in an EDP Symposium to examine the risks associated with mergers and acquisitions. To gain as broad a perspective as possible, various authorities, including agency regulators involved in the applications process, senior management responsible for information system conversions and consultants were invited to share their experience on the subject. The symposium participants addressed areas of concern, identified risks associated with mergers and acquisitions, and prepared conclusions and recommendations.

Findings

Historically, financial institutions have acquired significantly smaller institutions and have integrated the acquired institution into an existing organizational structure. In the past several years financial institution regulators have seen the consummation of mergers and acquisitions which have necessitated the development of new and complex information systems. One result is the consolidation of data processing systems and back office operations.

While a merger or acquisition may require the financial institution to engage in a system conversion, it should be noted that many conversions are unrelated to mergers or acquisitions. While there are risks associated with any conversion, well managed strong institutions have generally been able to overcome conversion problems successfully while weaker institutions have been adversely affected. Financial institutions have encountered unanticipated problems in the conversion process that have had implications throughout the institution. These include:

- An adverse impact on profitability;
- The reporting of inaccurate financial information to regulatory agencies;

-
- The inability to reconcile general ledger accounts;
 - Management decisions based on inaccurate information; and
 - A negative impact on public confidence.

Documented cases involving conversion-related data processing problems which examiners have reported include the following:

- A large money center bank was unable to complete processing for 32,000 trades of government securities, resulting in an overdraft of \$32 billion at the Federal Reserve;
- A large holding company experienced a \$4 billion out-of-balance condition following a change in its check processing system;
- As the result of a faulty general ledger system conversion, a thrift institution chronically filed late and inaccurate regulatory reports, resulting in civil money penalties being assessed; and
- As the result of a faulty check processing system conversion, a thrift institution was forced to charge off unresolved bookkeeping differences equivalent to one year's net income.

Poorly planned mergers have also resulted in systems conversions that have extended beyond projected time frames, resulting in unanticipated expenses and/or unrealized cost savings. Traditionally, mergers and acquisitions were accomplished within the confines of existing systems and, with adequate pre-planning, were effected in a short period of time. In the current merger and acquisition environment, where mergers of equal size institutions are not uncommon, the potential for an unsuccessful conversion is greatly increased. A 1989 survey by Ernst & Young and Keefe, Bruyette & Woods, Inc. of 34 banks and bank holding companies with assets over \$6 billion which were involved in mergers and acquisitions showed that in mergers of equals, neither bank had the capacity to absorb the data processing and back office operations of the other. Additionally, in this type of transaction, institutions have been able to reduce data processing and operations expense by amounts substantially below projections. The survey also showed that most of the institutions had extensive experience with acquiring smaller financial institutions while only a few had been involved in a merger with another large financial institution.

Conclusions

Symposium participants concluded that the following factors increase the potential for an unsuccessful or problem conversion:

- Insufficiently detailed plans;
- Failure to commit necessary resources;
- Failure to retain personnel necessary to effect a successful conversion;
- Inadequate controls which result in reconciliation and system problems; and
- Inaccurate reports produced by information systems.

RECOMMENDATIONS

To minimize the risks associated with mergers and acquisition involving conversions of information systems, regulators should:

- Determine the impact of these activities on EDP and other examination strategies. Examples of significant EDP conversions include: major application changes, initial conversion to in-house operations, outsourcing major applications, operating systems enhancements, and data security revisions;
- Review the institution's EDP plans for effecting the merger or acquisition as part of the application process; and
- Monitor the status of merger and acquisition activities involving data centers under their supervisory authority.



Federal Financial Institutions Examination Council

**SP-9
April 1993**

Subject: Interagency Supervisory Statement on EFT Switches and Network Services

**To: Chief Executive Officers of all Federally Supervised Financial Institutions,
Senior Management of each FFIEC Agency, and all Examining Personnel**

Purpose

The purpose of this supervisory issuance is to alert the Board of Directors and senior management of financial institutions to the risks associated with switch and network services in retail electronic funds transfer (EFT) systems. This statement does not address wholesale or large dollar funds transfer systems such as FEDWIRE and CHIPS.

Definitions

A switch is a computer system that facilitates the transfer of electronic messages between terminal devices and the appropriate network participants. For example, it transmits an inquiry or transaction from an automated teller machine (ATM) or point-of-sale (POS) terminal to the depository institution that holds the customer's account. EFT terminals, processors, and switches can be configured in many different ways, depending on the participants' needs. The combination of interconnected terminals and computers is a network. Networks are sometimes operated by independent third party servicers.

Background

Financial institutions have increased the use of switch and network services to lower costs and improve competitive position. Many financial institutions are sharing resources or using outside servicers, including non-financial companies, to provide EFT services. Such services include POS, ATM, and bill payment. Industry marketing efforts are promoting additional shared retail services, such as automated clearing houses (ACH), stored value cards, and credit card authorization.

EFT switches and network processing systems have expanded traditional methods of consumer banking, e.g., deposit, withdrawal, and obtaining credit. These systems provide customers with regional or nationwide access to their funds.

Some financial institutions are required by state law to share these services. Others voluntarily share them on a regional, national, or international basis.

Examples of shared EFT switch and network services include:

- A multi-bank holding company network servicing affiliated institutions;
- A network formed and shared by different types of financial institutions; and
- A non-financial company's proprietary network shared with financial institutions for a fee.

Regardless of the types of services offered or systems being used, there are inherent risks in switch and network services.

Concerns

The increasing use of switches and networks raises certain concerns for participants:

- **OPERATIONAL FAILURE:** System failure or service interruption, which may be caused by a disaster, could impact all connected financial institutions and could cause an erosion of consumer confidence;
- **SETTLEMENT FAILURE:** Network participants could fail to make required settlement payment, resulting in significant financial losses; or, the processor could fail to provide necessary settlement records, forcing participants to reconstruct transactions;
- **FINANCIAL FAILURE:** The switch servicer could experience sudden financial problems that may adversely impact all connected financial institutions;
- **DOLLAR LIMITS:** The network's dollar limits, such as those applied to withdrawals, may be different from the limits the institution established;
- **AUDIT COVERAGE:** Audits may not sufficiently cover internal controls, enforcement of standards, and review of transactions processed;
- **CONTRACTS:** Poorly written contracts may inadequately define participants' liabilities and responsibilities and expose financial institutions to potential loss.

Summary

The Board of Directors and senior management of financial institutions are responsible for:

- Ensuring that controls covering the switch processing environment are adequate. Alternatives to accomplish this objective include qualified internal or external auditors, or consultants specializing in this area. The results of these evaluations, and management's efforts toward correction, need to be documented in Board minutes.
- Ensuring that contracts for switches and network services are reviewed by legal counsel and meet minimum regulatory contract servicing guidelines. The guidelines are detailed in the FFIEC Interagency Statement on EDP Service Contracts (SP-6) and the FFIEC EDP Examination Handbook.
- Ensuring that settlement procedures do not pose undue risk to their institutions and that network rules adequately address actions that would be taken in the

event that a participating institution fails to settle.

The appendix to this statement provides controls that should be in place in an EFT switch or network services environment.

SP-9 - APPENDIX

Control Objectives

Control for a safe and sound EFT network switching environment should address the following items. These objectives apply to all EFT switches and network servicers regardless of ownership:

Management:

- Written, approved, and enforced policies and procedures covering personnel, security controls, operations, and disaster recovery;
- Adequate segregation of duties and responsibilities;
- Periodic control evaluations of the switch and network;
- Daily settlement of switch activity and balancing of network activity, and periodic verification of fee distribution;
- Contracts that identify the responsibility and liability of all parties (e.g., timely presentment of returned items and appropriateness of fees and surcharges); and
- Adequate fidelity and business interruption insurance.

Security:

- Physical access restrictions;
- Encryption of critical data elements (e.g., personal identification code);
- Adequate management of encryption keys used in software;
- Software access controls including the program library, data files, and the network;
- Controlled access to positive and negative card files, used to authorize transactions; and institution control files (ICF) or institution parameter blocks (IPB), used to store institution-specific processing criteria; and
- Captured card procedures.

Operations:

- File backup and disaster planning including telecommunications;
- Audit trails sufficient to trace transactions through the system;
- Stand-in processing (having the cardholder data available at the switch for authorization) procedures should be available in the event of processor downtime, including the handling of positive balance files (PBF) and cardholder authorization systems (CAS);
- Restart and recovery procedures to ensure the continuity of transaction processing in the appropriate sequence;
- Controls over the embossing, encoding and distribution of access devices; and
- Controls over the generation of cardholder personal identification codes (PIC) and communication of PICs to cardholders.



Federal Financial Institutions Examination Council

**SP-10
December 1993**

Subject: Control And Security Risks in Electronic Imaging Systems

To: Senior Management of Each FFIEC Agency and All Examining Personnel

Purpose

This issuance advises the senior management and examining personnel of each FFIEC agency of risks associated with electronic imaging systems in financial institutions.

Definition

Electronic imaging systems is a term that describes the technology used to capture, index, store and retrieve electronic images of paper documents.

Background

Technological advances in document scanning and optical character recognition are replacing the traditional paper storage systems in financial institutions. These systems incorporate new technologies such as optical disk storage, high resolution displays, document scanners, and laser printers to capture, store and print documents. Once stored in electronic form, the documents can be accessed throughout the organization. Image systems can range from small systems supporting a business function or department with a few users, to large systems or networks supporting multiple departments with hundreds of users.

Imaging systems replace the handling, distribution and storage of paper documents with electronic images. They are generally grouped into two types of systems: Document Management Systems and Item Processing Systems.

Document Management Systems

Document management imaging systems automate the flow of paper documents processed by departments and offices in a financial institution. These applications are referred to as "low-speed" imaging systems as documents contained in office or customer file folders are scanned one at a time. The process consists of capturing original documents in electronic form on a low-speed scanning device, entering additional data and text into the record via keyboard entry, indexing the file folder and documents in a computer data base, and storing the folder on electronic storage media. Documents can then be displayed on a computer terminal, processed, or printed at work stations throughout the organization. These systems allow for the automatic routing of electronic documents to those individuals involved in the review or decision making process. They can also

route documents or file folders for quality control reviews.

Document management systems account for the majority of imaging systems in financial institutions today. Examples of business functions where original documents (loan applications, customer correspondence, etc.) are being converted to imaging systems to improve processing and customer service are:

- customer service account inquiries
- student loan processing
- loan/mortgage servicing applications
- IRA/Keogh files
- trust files
- signature verifications
- accounts payable

Item Processing Systems

Item processing imaging systems automate check or remittance processing applications on reader-sorters or similar high speed capture equipment. Images of transaction items are captured and stored for later use in encoding documents and exception processing. Item processing imaging systems require special attention to the quality and readability of the imaged documents. These high speed systems are relatively expensive to install as they require special scanning equipment, expanded storage capacity, and complex software programs to convert documents into readable electronic images.

Examples of item processing applications where transaction documents are converted to images for processing are:

- proof-of-deposit
- sales draft (credit card/POS) processing
- remittance processing
- account reconciliation processing
- statement rendering

Control and Security Risk Areas

The replacement of paper documents with electronic images can have a significant impact on the way that an institution does business. Many of the traditional audit and security controls for paper based systems may be reduced or absent in electronic document workflow. New controls must be developed and designed into the automated process to ensure that information in image files cannot be altered, erased or lost.

Risk areas that management should address when installing imaging systems, and that examiners should be aware of when examining an institution's controls over imaging systems, are listed below:

Planning – The lack of careful planning in selecting and converting paper systems to document imaging systems can result in excessive installation costs, the destruction of original documents, and the failure to achieve expected benefits. Critical issues such as converting existing paper storage files, integration of the imaging system into the organization workflow, and equipment backup and recovery procedures should be addressed to avoid reduced customer service and business interruptions.

Audit – Imaging systems may change or eliminate the traditional controls, and checks and balances inherent in paper based systems. Audit procedures may have to be redesigned, and new controls designed into the automated process. Audit departments should be sufficiently involved to ensure that electronic document workflows include appropriate audit controls and audit trails.

Redesign of Workflow – Institutions generally redesign or reengineer workflow processes to benefit from imaging technology. New jobs or functions are identified and others eliminated. Changes may range from the redesign of forms to the reorganization of departments. Traditional controls such as time/date stamps, control numbers, review signatures, etc. may be replaced by limiting access to imaged documents, automated logs that report document access and retrieval information, etc. The absence of these, and other automated controls, may result in increased risks for the institution.

Scanning Devices – Scanning devices are the entry point for image documents and a significant risk area in imaging systems. Scanning operations can disrupt workflow if the scanning equipment is not adequate to handle the volume of documents, or the equipment breaks down. The absence of controls over the scanning process can result in poor quality images, improper indexing, and incomplete or forged documents being entered into the system. Factors that should be considered in an imaging system are quality control over the scanning and indexing process, the scanning rate of the equipment, the storage of images, equipment backup, and the experience level of personnel performing the scanning function.

Indexing – Poorly designed imaging system indexes can result in lost or inaccessible documents. Proper indexing of scanned documents is critical to later retrieval, and establishing access levels to individual documents and file folders. The integrity of indexes must be carefully maintained to ensure access to all documents and protection from unauthorized modification. The indexing method can affect the security administrator's ability to restrict access to documents or file folders. The institution should maintain automated journals and audit trails of document access and modifications to customer records.

Software Security – Security controls over image system documents are critical to protect institution and customer information from unauthorized access and modifications. The integrity and reliability of the imaging system database is directly related to the quality of the controls over access to the system. Software security and security administrator functions are essential to prevent unauthorized alterations to stored documents.

Contingency Planning and Backup Procedures – Since more than 100,000 documents may be stored on a single optical disk, the loss of electronic image files or storage media can severely impact business operations if back-up electronic or paper files are not readily available. Contingency planning and back-up storage procedures for imaging system documents should follow generally accepted practices for data processing and management information systems.

Training – Inadequate training of personnel scanning documents can result in poor quality document images and indexes, and the early destruction of original documents. The installation and use of imaging systems can be a major change for department personnel. They must be adequately trained to ensure quality control over the scanning and storage of imaged documents, as well as the use of the system to maximize the benefits of converting to imaging systems.

Legal Issues – Case law on the admissibility of electronic image as evidence has not yet been established by the courts. Although precedent has been established on related electronic documents such as facsimile, microfilm, and photocopies, the courts have not addressed the authenticity of electronic images of original documents. Institutions installing imaging systems

should carefully evaluate the legal implications of converting original documents to image, and the subsequent destruction of the original documents.

Conclusion

Imaging systems offer institutions benefits in streamlining department and office workflow processes, reduced storage and retrieval costs, and improved customer service by automating customer files and correspondence. These systems present new concerns and challenges for examiners and board of directors who must ensure that the risks are addressed by the institution's management.



Federal Financial Institutions Examination Council

**SP-11
January 1995**

**Subject: Enhanced Supervision Program for Multidistrict Data
Processing Servicers (MDPS)**

To: Senior Management of Each FFIEC Agency and All IS Examining Personnel

Objective

To establish guidelines to improve the supervision of and communication with the independent data processing service vendors in the Multidistrict Data Processing Servicers program.

Background

The MDPS examination program presently covers 17 nonbank EDP vendors that provide key data processing services to more than half of the federally insured depository institutions. In recent years, many of the country's larger depository organizations have outsourced their EDP operations which has increased further the industry's dependence on outside service bureaus. Most vendors service institutions through regional data centers. The institutions depend on the quality and continuity of these services to conduct their business. Disruptions in services at a single vendor, as a result of either financial or operational conditions, could cause substantial systemic risk in the industry.

The core element of the interagency MDPS program continues to be the on-site Information Systems examination. The FFIEC's Interagency EDP Examination, Scheduling and Distribution Policy, as amended in 1991, identifies the frequency for examinations under the MDPS program. Those vendors, rated 1 or 2 are examined on a 24 month examination cycle; vendors rated 3, on an 18 month cycle; and vendors rated 4 or 5, on a 12 month cycle. As part of each examination, the agency-in-charge is responsible for formulating and implementing a supervisory strategy.

Enhanced Supervisory Program (ESP)

The ESP supplements existing on-site examinations with interim reviews of material changes in the vendor's activities and condition. The ESP should allow each agency to more promptly recognize and supervise risks associated with the concentration of services in vendors.

The interim reviews will follow up on matters from the previous examination, assess major changes (e.g. in the vendor's business plan, the number and type of financial institutions serviced, corporate/management structure, financial condition, and hardware and software), and plan subsequent reviews and examinations. The scope and frequency of the interim reviews will vary depending on the condition and/or degree of change in the vendor. However, vendors that are on a 24 month examination cycle are expected to receive a minimum of two interim reviews and vendors on 12 or 18 month cycles are expected to receive at least one interim review.

Reviews may be conducted through correspondence, telephone interviews, and/or other requests

for information if the agency-in-charge is able to obtain the information necessary to evaluate the vendor's condition and stay abreast of material changes in its activities and operations without going on-site to collect the information. Interim reviews for vendors rated 3, 4, or 5, and those experiencing major changes in their activities and operations, are expected to be on-site visits.

If visits are necessary they will be conducted at the corporate headquarters of the vendor and ordinarily will not include branch or subsidiary data center sites. However, if necessary, examiners may visit additional sites. If the agency-in-charge requires assistance from examiners from other agencies, the Subcommittee should be informed as early as possible to facilitate coordination.

Reporting

The agency-in-charge (AIC) will be responsible for preparing a brief summary memorandum documenting findings, conclusions, and recommendations from each interim review. That memorandum is an internal document and is not intended for distribution. The memorandum will be provided to the Subcommittee and shared with the agencies, as appropriate. The memorandum should include a brief discussion of:

- (1) The vendor's progress in addressing recommendations presented in the last examination;
- (2) The vendor's progress in addressing recommendations presented in selected internal and external audit reports;
- (3) Any deterioration in financial condition or other matters that threaten the vendor's viability or its ability to continue to provide uninterrupted service;
- (4) Recommendations regarding frequency, timing, scope, and locations of future reviews and examinations; and
- (5) A listing of participating examiners, agencies and duration of participation.

At the conclusion of the interim review, a brief overview of the examiner's conclusions and any material findings or recommendations should be discussed with the vendor. Unless the agency-in-charge considers it necessary, there is no need for a formal close-out meeting with the vendor's directors or their designated compliance or audit committees.

If the agency-in-charge prepares separate written correspondence for the vendor, a copy of the letter will be provided to the Subcommittee.

Role of the Information Systems Subcommittee

In order for the Subcommittee to provide for consistency in the conduct of the program and to assure effective coordination and scheduling of examiner resources, the AIC will provide the Subcommittee with a strategy for supervising the vendors. That strategy will include information on the agency's proposed schedule and scope for the conduct of examinations and anticipated interim reviews. The Subcommittee will provide guidance to the member agencies in their conduct of interim reviews.

In developing this program, the Subcommittee has designed the frequency, scope, and reporting requirements for interim reviews so as not to require significant additional examiner resources for the supervision of vendors. The Subcommittee anticipates that the interim reviews will permit the AIC to be more familiar with the vendors and, therefore, will reduce the time spent on the examination.

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-Appling 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.

FRB IS EXAMINATION POLICY ISSUANCES CHAPTER 27 (SUPERVISION AND REGULATION DIVISION)

(FILE NAME ON DISK # 2 = S3C27.WPD)

TABLE OF CONTENTS

Number	Date	Subject
SR-81-678	03-27-81	Alternate Year Examination Program
SR-81-703	07-13-81	Examination Responsibility for Remote Job Entry Sites/Interagency Rating System EDP Report of Examination
SR-82-42	08-16-82	EDP Examination Guidelines for Facilities Management Operations
SR-84-19	07-24-84	Offsite Electronic Facilities
SR-86-39	11-07-86	Frequency and Scope of Specialized Examinations
SR-88-2	01-21-88	End User Computing <i>See FFIEC Policy SP-3 for details.</i>
SR-88-33	11-30-88	Supervisory Policy on Large Scale Integrated Financial Software Systems <i>See FFIEC Policy SP-4 for details.</i>
SR-88-37	12-28-88	Disclosure of Numeric Composite Examination and Inspection Ratings to Examined/Inspected Institutions
SR-89-16	08-01-89	Interagency Policy on Contingency Planning for Financial Institutions <i>See FFIEC Policy SP-5 for details.</i>
SR-89-21	09-26-89	EDP Examination Data Base
SR-90-5	01-24-90	Interagency Statement on EDP Service Contracts for Financial Institutions <i>See FFIEC Policy SP-6 for details.</i>
SR-91-21	10-11-91	EDP Interagency Examination, Scheduling and Distribution Policy <i>See FFIEC Policy SP-1 for details.</i>
SR-93-25	05-14-93	Interagency Supervisory Statement on EFT Switches and Network Servers

See FFIEC Policy SP-9 for details.

SR-94-2 01-13-94

Electronic Imaging Systems

See FFIEC Policy SP-10 for details.

SR-95-7 02-09-95

Enhanced Supervision Program for Multiregional Data Processing Servicers

See FFIEC Policy SP-11 for details.

SR-95-48 11-09-95

Fedwire Third-Party Access Policy

See FRRS 9-1016 (Federal Reserve Regulatory Service)

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 81- 678
March 27, 1981

TO THE OFFICER IN CHARGE OF SUPERVISION AT EACH FEDERAL RESERVE BANK

On March 18, 1981 the Board approved the alternate year examination program (AEP) as System policy for the commercial examination of State member banks. The AEPs would also include trust and electronic data processing examinations if the State has sufficient examination expertise, but would not include consumer affairs and CRA examinations. Under the program, certain mutually agreed upon State member banks that are relatively free of problems would be divided into two groups, with each group being examined in alternate years by the Reserve Bank and the State. Thus, a particular bank would be examined by the Reserve Bank in one year, the State in the next and so on. The program will not restrict the supervisory prerogatives or alter the supervisory responsibilities of either the Federal Reserve or the States. While the program is meant to encourage Federal Reserve-State cooperation, any bank may be removed from the program and examined at any time by either agency, and either agency can meet with a bank's management or board of directors or initiate supervisory action whenever deemed warranted.

Adoption of AEP amends the Federal Reserve's examination frequency policy by permitting the time between System examinations of relatively trouble-free banks to be extended from 18 months to 24 months, provided a State examination under AEP is conducted in the interim. In some instances, judgment may be exercised if commencing a Federal Reserve examination and the bank's condition does not warrant an immediate on-site Federal Reserve examination. Banks requiring more than normal supervisory attention, banks not included under the alternate schedule for reasons of size and certain other banks at the discretion of either agency will continue to be examined under existing frequency policies.

The program will be implemented on a state-by-state basis with those States that have an interest and adequate examination staffs. In determining the adequacy of state examination programs, Reserve Banks should consider the level of expertise and experience of state examiners, the size of the examination force, and the quality and scope of state examinations. Generally, commercial examinations should include an analysis of all determinants of safety and soundness, an evaluation of internal systems and management, a review of the accuracy of supervisory reports and an assessment of compliance with general banking laws, regulations and supervisory policies. Reserve Banks should cooperate with the States in order to enhance the State examiners' understanding of Federal laws and regulations, especially those designed to limit risk-taking and extensions of credit to affiliates and insiders. If a state is split between more than one Reserve District, the two Reserve Banks should be consistent in determining whether it would be appropriate to conduct the AEP with that state and should negotiate an AEP arrangement with the State on that basis. If two Reserve Banks cannot reach a consensus on the State, the Reserve Banks should send to Board staff a written account of why such a disagreement exists. The situation will then be presented to the Board's

Committee on Banking.

Supervision and Regulation for resolution. States that have a statutory annual examination requirement might be able to participate in AEP and still satisfy the requirement by sending a representative along with the Reserve Bank's examination team.

The program will be initiated through a memorandum of understanding or letter agreement between the Reserve Bank and the State. (A proposed minimum agreement format is attached.) Aside from provisions listed in the attachment, the format of AEP agreements will be flexible to accommodate particular Reserve Bank and/or State needs and changing conditions within the banking industry. Some examples of such provisions might include: a) a size criterion for including banks in AEP if either agency's resource limitations would preclude its conducting independent examinations of larger institutions; b) on-site representation of one agency during an alternate examination being conducted by the other agency; and c) agreement to assist the State examiners in understanding Federal banking laws and regulations. Reserve Banks should notify the Projects and Planning Section when discussions regarding AEP are started with any State banking department and should send Board staff a copy of the draft agreement negotiated with the State banking department prior to final implementation.

The Reserve Bank and the State banking department should meet in advance to mutually agree on the list of banks whose examinations are to be alternated in the subsequent examination period. Further meetings should be held periodically to add or delete banks from the list if warranted by changing financial conditions. The list of mutually agreed upon State member banks should be accorded confidential treatment by the Reserve Bank and the State banking department. In deciding whether to include large banks with significant shared national credits (SNCs) or loans involving country risk, Reserve Banks should carefully consider the supervisory treatment the State accords these areas. States should be encouraged to participate in these programs or to incorporate classification schemes consistent with the SNC and country risk programs. Reserve Banks should stand ready to assist States in these areas if necessary. State member banks included under the AEP normally would be rated CAMEL composite 1 or 2. Nonetheless, a particular bank rated composite 1 or 2 might be excluded from AEP if the Reserve Bank or State banking department felt it would be necessary to examine that bank under the existing examination policy for a specific reason relating to the nature of the bank's business, a particular finding regarding the bank's operation, or the bank's size. In addition, improving composite 3's could be included, while deteriorating composite 1's or 2's could be excluded.

The initial phase of the program would run for two years to allow one full cycle of alternated examinations to be conducted. Within this two-year period, all banks included in AEP should be examined at least once by the Reserve Bank. Thereafter, the program could be reviewed and extended in a manner mutually agreeable to the Reserve Bank and the State. This is not to imply that the agencies would meet or communicate only to determine whether to continue the program; rather the program should be established on a fundamental understanding that timely communication and exchange of information and close cooperation are essential to the success and continuance of the AEP. While the program may be terminated anytime at the discretion of either agency, Reserve Bank concerns about how the program is progressing or working should be discussed with Board staff before approaching the State for the purpose of limiting or possibly terminating the program.

Due to the extension of time between Federal Reserve examinations of AEP banks, Reserve Banks should closely monitor the financial condition of such banks through the financial surveillance and screening programs. Such activities and off-premise analyses should be stepped up and strengthened where necessary. CAMEL ratings should be updated between Federal Reserve examinations whenever there is a material change in financial condition based upon State examinations, call and

income and dividend reports and other relevant information. SR-665 outlines procedures to be followed to effect a change in rating between System examinations.

Reserve Banks should receive and analyze all examination reports from the States which are prepared on banks included in AEP. A written analysis of each State examination report should be forwarded to Board staff along with a copy of the examination report.

Implementation of the program will foster greater cooperation and joint supervisory actions, but is not meant to limit the Reserve Bank's supervisory responsibilities, prerogatives or flexibility. The program should result in a reduction of duplication and the elimination of separate Federal and State examinations of certain sound banks in one year and thereby produce some budget savings. However, in many instances it will be necessary to use these savings in order to strengthen the on-site coverage of bank holding companies and the off-premise surveillance and analysis activities that are required to implement the AEP and the recently enacted examination frequency policy.

Questions concerning the program as well as notification of the initiation or conduct of discussions with States should be directed to Richard Spillenkothen (x2594) or Rita Corwin (x2740). It is recognized that implementation of AEPs may have to be accomplished over time by gradually increasing the number of banks whose examinations are alternated as both the Reserve Bank and the State gain experience in participating in the program.

/s/John E. Ryan
Director

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 81-703
July 13, 1987

TO THE OFFICER IN CHARGE OF SUPERVISION AT EACH FEDERAL RESERVE BANK

We present the following guidelines in response to various questions that have been raised by Reserve Districts regarding the EDP Examination Program,

Interagency Policy Statement (SR-475)-Examination responsibility for Remote Job Entry (RJE) sites. Recently, many financial institutions have entered into RJE computer servicing arrangements. Unlike conventional types of computer servicing arrangements, RJE's allow data processing operations (input/output) to be conducted at financial institutions remotely located from the main computer center. In these cases, the regulatory agency that supervises the financial institution in which the RJE is located should conduct the EDP examination of the RJE site. Alternate examination arrangements can be made between the Federal regulatory agencies, however, such arrangements should be fully discussed among the agencies at the district/regional level prior to conducting the examination.

Interagency Rating System (SR-507)-Performance rating for each function. The rating system is based on an evaluation of the four critical functions of a data Processing operation: audit, management, systems and programming and computer operations. Regardless of whether the organization being examined performs each function, a numerical rating must be assigned to each function during the examination.

Specifically, audit and systems and programming ratings are frequently omitted in the Administration section of the EDP Report of examination. As examples:

- (1) An organization may not have an internal auditor, however, an audit function should exist. To formulate an EDP audit performance rating, determine if appropriate audit standards and procedures have been developed and are being followed.
- (2) Regardless of the amount of in-house programming an organization conducts, controls should be maintained over computer software and program modifications. To evaluate the performance of the systems and programming function, examiners should review areas such as software controls, security and backup of software documentation, system enhancement and program change procedures and vendor support.

**EDP Report of Examination (SR-640)-Report pages
and sections that are often incorrectly prepared**

COVER

- (1) Use the standard interagency cover page for all EDP Reports of Examination. (State member banks, independent data processing companies, subsidiaries or affiliates of bank holding companies, bank service corporations, etc.)
- (2) List the "Agency" name for the Federal Reserve System as THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM.
- (3) State the appropriate Federal Reserve Bank name following the examiners name. (Only lead examiners should be named on the cover page.)

ADMINISTRATIVE SECTION

- (1) Page A: LIST each function rating as well as the composite rating for prior examination information.
- (2) Page C: Systems Description-Include the core storage capacity, name of the operating system and programming language in the hardware and software descriptions.
- (3) Page C: Organizational Structure-Report the total number of employees that are employed in the financial Institution or data center. In addition, specify the number of persons that work in the computer operations and systems and programming functions of the organization. (NOTE: The total number of employees should be greater than the sum of both functions.)
- (4) Page C: Ownership-state any affiliation a bank or data center may have with another bank or bank holding company. (Provide the name and location.)

/s/John E. Ryan
Director

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 82-42(FIS)
August 16, 1982

TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK

SUBJECT: EDP Examination Guidelines for Facilities Management Operations

The Interagency EDP Examination Subcommittee has developed the following guidelines for uniform report preparation and distribution of data centers operating under a facilities management agreement. The guidelines are being distributed to each District/Region of the participating agencies.

DEFINITIONS

For the purpose of these guidelines:

- An Examined Organization is a financial institution or data center that contracts another organization's employees and/or computer equipment to develop, implement and operate a data processing function on its behalf.
- A Facilities Management (FM) Organization is an organization responsible for operating all or part of a data processing function under the provisions and agreements set forth in a written contract.

REPORT PREPARATION

The names and locations of both the examined organization and the FM organization should be reported on the cover of the EDP examination report as follows:

- Record the name and location of the examined organization in the areas marked (Data Center) (City) (County) and (State).
- Record the name and location of the FM organization (as it appears on the contract) on the line below the date of the examination.
- Include financial statements of the FM organization and the examined organization (unless it is a financial institution) in the EDP examination report. Examiners should analyze the financial condition of both entities and include relative comments on the Administrative Remarks page of the confidential section.
- Describe the organizational structure and processing arrangements (hardware, software,

personnel) in the confidential section.

REPORT DISTRIBUTION

Distribute a copy of the EDP examination report to the board of directors of the examined organization and the FM organization.

- Unless there are unusual circumstances, an unabridged copy of the report should be sent to the examined organization.
- Comments which specifically address the examined organization only should be edited from the report distributed to the FM organization.

/s/John E. Ryan

Director

Cross References: SR-640

Supersedes: N/A

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

**DIVISION OF BANKING
SUPERVISION AND REGULATION**

**SR 84-19(FIS)
July 24, 1984**

TO THE OFFICER IN CHARGE OF SUPERVISION AT EACH FEDERAL RESERVE BANK

In 1975 the Board issued instructions (S-2285) to the Reserve Banks regarding offsite electronic facilities. The instructions state in part:

"The Board has recently considered a request by a State member bank to establish offsite electronic facilities. Many such facilities have the capacity to accept deposits, make loans, or pay checks, and have become generally known as cash dispensers, automated tellers, and point-of-sale terminals."

"In view of the legal and policy issues raised by the establishment or use of offsite facilities that provide any or all of the above described services, the Board has determined that, at this time, a State member bank desiring to establish or use an offsite electronic facility described above shall inform the Federal Reserve Bank in its district thirty days prior to the establishment or utilization of such facility. Where applicable State law or the appropriate State bank supervisory authority has permitted or approved deployment of the proposed offsite facility, and where the Reserve Bank does not notify the applicant of its objection to the establishment or use of the facility within the 30-day period, the member bank may take action to establish or use such facility."

The Board's Rules of Procedures provide that an application by a State member bank for establishment of a domestic branch or other facility (offsite electronic facility) that would be authorized to receive deposits is subject to CRA publication requirements.

While the above quoted instructions remain outstanding, some confusion has arisen as to the interpretation of the instructions. The Board recently authorized Board Staff to join with the Comptroller of the Currency in filing an amicus brief in a court case involving the branch status of an automatic teller machine (ATM). The Board took the position that if a bank (1) did not own or rent a particular ATM and (2) if that ATM was shared with other institutions, then the ATM would not be considered a branch requiring notification. Offsite electronic facilities not satisfying both of these tests should be regarded as a branch of each bank that uses the facility.

When a state member bank joins a network that meets both of the above tests, it should advise the Reserve Bank of such action by letter even though no branch application is required. Moreover, the

network should advise the Reserve Bank on a quarterly basis of the location of each facility added to the network.

State member banks in your District should be advised of these procedures if they vary from your current practices.

/s/John E. Ryan
Director

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 86-39 (SA)
November 7, 1986

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: Frequency and Scope of Specialized Examinations

As you know, the new Frequency Guidelines for Commercial and Bank Holding Company Examinations (SR 85-28 (FIS)) did not address specialized examinations, such as examinations for trust institutions (bank trust departments and trust companies), registered transfer agents, registered clearing agents, EDP operations and municipal securities dealers. Staff has now completed a detailed review of the frequency requirements for these specialized examinations and individualized frequency guidelines, which take into account the differences in the nature of these specialized areas, have been adopted as set forth below. Tables presenting these frequency and scope requirements are attached.

More frequent examinations should, of course, be scheduled by Reserve Banks if necessary.

Trust Examinations

A trust institution rated U.I.T.R.S.¹ composite 1 or 2 at the last examination with total discretionary assets greater than \$500 million will be subject to a full-scope examination every two years to be conducted either by the Federal Reserve independently or jointly with the State, provided that the Reserve Bank has no reason to believe that there has been a material change and/or deterioration in the institution's management, condition, or character of business since the last examination, and all substantive issues commented upon in the last examination report have been satisfactorily resolved. A trust institution rated U.I.T.R.S. composite 1 or 2 with total discretionary assets between \$100 and \$500 million will be subject to a full-scope examination every three years by the Federal Reserve, provided an acceptable State examination is conducted in the interim (otherwise every two years). A trust institution rated U.I.T.R.S. composite 1 or 2 with total discretionary assets less than \$100 million will be subject to a full-scope examination every four years by the Federal Reserve, provided an acceptable State examination is conducted in the interim (otherwise every two years).

A trust institution rated U.I.T.R.S. composite 3 at the last examination with total discretionary assets greater than \$100 million will be subject to an annual full-scope examination to be conducted either by

¹ U.I.T.R.S. refers to the rating system used by the federal supervisory agencies to assess the condition of trust institutions (F.R.R.S. 3-1576).

the Federal Reserve independently or jointly with the State. A trust institution rated U.I.T.R.S. composite 3 with total discretionary assets less than \$100 million will be subject to a full-scope examination every two years to be conducted either by the Federal Reserve independently jointly with the State.

A trust institution rated U.I.T.R.S. composite 4 or 5 at the last examination must be examined on a twice-a-year basis (every six months) until rated 3 or better, at least one of these two examinations must be full-scope and both must be conducted by the Federal Reserve independently or jointly with the State.

Full-scope, limited scope or targeted examinations should be conducted more frequently if deemed necessary by the Reserve Bank.

The trust activities of State chartered banks or trust companies applying for membership in the Federal Reserve System are to receive a full-scope examination by the Federal Reserve before membership is granted. Similarly, a full-scope trust examination by the Federal Reserve, independently or with the State, will be required within 12 months: following (1) the formation of a de novo State member bank or trust company, or (2) the change in control of a state member bank or trust company.

Transfer Agent Examinations²

A registered transfer agent rated TA composite A³ at the last examination, and servicing more than 500 issues, will be subject to a full-scope examination every two years, provided that the Reserve Bank has no reason to believe there has been a material change: and/or deterioration in the institution's management, condition, or character of business since the last examination, and all substantive issues commented upon in the last examination report have been satisfactorily resolved. Transfer agents rated TA composite A and servicing less than 500 issues will be subject to a full-scope examination every three years. Transfer agents rated TA composite B must be examined annually, and transfer agents rated TA composite C must be examined every six months. Newly registered transfer agents are to receive a full-scope examination by the Federal Reserve within 12 months of registration.

Registered Clearing Agency Examinations

All registered clearing agencies will be subject to full-scope examinations annually by the Federal Reserve.

Electronic Data Processing Examinations

The revised guidelines contained in Table A also apply to EDP Examinations conducted in state member banks⁴ and Edge Corporations. Those institutions rated EDP⁵ composite 1 or 2 at the last

² A bank's transfer agent activities are a separate service provided to customers, the size or volume of which is not necessarily related to commercial or trust department activities. Additionally, some organizations subject to Federal Reserve supervision are not organized as banks, but rather as, for example, securities processing subsidiaries of bank holding companies. Therefore, an examination frequency based on trust asset size is considered inappropriate. Instead, frequency is based on the total number of issues serviced as transfer agent.

³ TA rating refers to the rating system used by the Federal Reserve to assess the condition of registered transfer agents (F.R.R.S. 3-1577).

⁴ Including facilities management operations unless examined under the MDPS schedule.

⁵ EDP rating refers to the rating system used by the federal supervisory agencies to assess the condition of EDP operations (F.R.R.S. 3-1515).

with assets greater than \$500 million are subject to a full-scope examination every two years to be conducted either by the Federal Reserve independently or jointly with the State, provided that the Reserve Bank has no reason to believe that there has been a material change and/or deterioration in the institution's management, condition, or character of business since the last examination, and all substantive issues commented upon in the last examination report have been resolved satisfactorily. Institutions rated EDP composite 1 or 2 with total assets between \$100 and \$500 million are subject to a full-scope examination every three years by the Federal Reserve, provided an acceptable State examination is conducted in the interim (otherwise every two years). An institution rated EDP composite 1 or 2 with total assets less than \$100 million is subject to a full-scope examination every four years by the Federal Reserve, provided an acceptable State examination is conducted in the interim (otherwise every two years).

State member banks and Edge Corporations rated EDP composite 4 or 5 at the last EDP examination must be examined on a twice-a-year basis (every six months) until rated 3 or better; at least one of the two examinations must be full-scope and both must be conducted by the Federal Reserve independently or jointly with the State.

State member banks and Edge Corporations rated EDP composite 3 at the last EDP examination with total assets greater than \$100 million will be subject to an annual full-scope examination to be conducted either by the Federal Reserve independently or jointly with the State. An institution rated EDP composite 3 with total assets less than \$100 million will be subject to a full-scope examination every two years to be conducted either by the Federal Reserve independently or jointly with the State.

State member banks and Edge Corporations rated EDP composite 3 at the last EDP examination with total assets greater than \$100 million will be subject to an annual full-scope examination to be conducted either by the Federal Reserve independently or jointly with the State. An institution rated EDP composite 3 with total assets less than \$100 million will be subject to a full-scope examination every two years to be conducted either by the Federal Reserve independently or jointly with the State.

Independent servicers, bank service corporations and other data centers rated EDP composite 1 or 2 that process major applications for state member banks are subject to an 18 month examination cycle. Annual examinations are to be conducted in data centers rated EDP composite 3. Data centers rated EDP composite 4 or 5 are to be examined on a twice-a-year basis (every six months); one of the two examinations may be a limited-scope or targeted examination.

Newly organized data centers must be examined within one year of the start of operations.

Multi-regional Data Processing Servicers (MDPS) with an EDP composite rating of 1 or 2 are to be examined within an 18 month time frame. The examinations are to be conducted concurrently with the lead bank, where possible. Institutions with an EDP composite rating of 3, 4, or 5 require ongoing supervision. No more than 12 months should elapse between examinations.

Full-scope, limited scope or targeted examinations may be conducted more frequently if deemed necessary by the Reserve Bank. For each of these types of examinations a report is to be completed and submitted to the examined institution. Reserve Banks are asked to send a copy to the Clearing Unit at the Board.

Municipal Securities Dealers

Municipal securities dealer activities should be examined at least once every 24 months, as required by Municipal Securities Rule making Board (MSRB) rules, provided that: (1) as of the date of the last examination there were no significant deficiencies in the bank's compliance with MSRB rules, Board rules, or related securities laws; (2) management of municipal securities dealer activities is believed to be capable and stable; and (3) the Reserve Bank has no reason to believe that there has been a major change in the type and scope of activities conducted by the dealer department operations since the last examination.⁶ Dealer banks failing to meet the preceding criteria should be examined on an annual, or even more frequent, basis depending on the severity of compliance problems or changes in circumstances.

With respect to de novo municipal securities dealer operations, Reserve Banks should attempt to conduct the first examination within six months of dealer registration. It is vital to promptly examine new entrants to the industry to ensure compliance with the panoply of MSRB and other rules governing these specialized activities.

Implementation of these procedures should begin with the scheduling of remaining 1986 examinations, where practicable. Since only nominal changes are involved and examination resource impact should not be adversely affected, full implementation should be achieved in 1987.

/s/Welford S. Farmer
Deputy Director

Attachments

CROSS-REFERENCE: SR-665, SR-678, SR-33, SR-729/TR-53 SR 85-28

SUPERSEDES: SR-665, SR-678, TR-33, SR-729/TR-53 (in pertinent part)

⁶ Currently, no state banking department examinations of municipal securities dealers are conducted, and thus there is no provision for Joint examinations of this activity.

TABLE A

FREQUENCY AND SCOPE OF EXAMINATIONS OF TRUST INSTITUTIONS AND EDP
EXAMINATIONS OF STATE MEMBER BANKS AND EDGE CORPORATIONS

Asset/ Rating	\$500 million and larger	\$100mm-500mm	\$100mm
1 or 2	Full-scope required Every two years (FR or Joint).	Full-scope (FR) required (FR) required every three years provided an acceptable state exam- nation is conducted in the interim. Otherwise Otherwise full-scope is Required every two years.	Full-scope (FR) required (FR) required every four years provided an acceptable state exam- ination is conducted the interim. full-scope is Required every two years.
3	Full-scope required annually (FR or Joint)		Full-scope required every two years (FR or Joint)
4 or 5	Required on a twice-a-year basis (every six months); one must be full-scope, one may be limited-scope or targeted. (Both must be FR or Joint)		

Special Characteristics:

1. New member banks or trust companies: Full-scope FR examination required before membership granted.
2. Change in control: Full-scope FR examination required within 12 months.

Notes:

1. Asset Size refers to total discretionary trust assets for purposes of the frequency of trust examinations.
2. A full-scope examination covers all areas of interest to the Federal Reserve in depth; a limited-scope examination will review all areas of activity covered by a full-scope examination, but less intensively; targeted examinations will focus intensively on one or two activities.
3. Joint examinations are conducted by the Federal Reserve and the State, simultaneously, generally with one joint report being prepared.

TABLE B
FREQUENCY AND SCOPE OF EXAMINATIONS OF TRANSFER AGENTS

Rating	Larger Institutions	Smaller Institutions
A	Full-scope required every two years.	Full-scope required every three years.
B	Full-scope required annually.	
C	Full-scope required on a twice-a-year basis (every six months).	

Special Characteristics:

1. Newly registered transfer agents: Full-scope FR examination required within 12 months.

Notes:

1. Larger institutions refers to those transfer agents which service 500 or more issues; smaller institutions refers to those which service less than 500 issues.
2. Currently, no state examinations of registered transfer agents are conducted, thus there is no provision for Joint examinations.
3. Certain special situations may warrant deviation from the above matrix, e.g., a large mutual fund custodial business. In these cases Reserve Banks maintain discretion in determining examination frequency, based upon considerations such as volume and nature of activity.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 88-2 (FIS)
January 21, 1988

TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK

SUBJECT: End-User Computing

The widespread use of microcomputers by financial institutions has provided end-users with direct access to sensitive and valuable bank data. The federal banking agencies are concerned, that in some financial institutions, the use of microcomputers may have out paced the implementation of controls. Accordingly, the agencies have agreed to alert institutions subject to their supervision to the risks associated with end-user computing and the appropriate controls for safe and sound processing of data within the microcomputer environment.

Please distribute the enclosed document on end-user computing to your examination staff and each State member bank in your district.

/s/Stephen C. Schemering
Deputy Associate Director

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 88-33(FIS)
November 30, 1988

TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK

SUBJECT: Supervisory Policy on Large-Scale Integrated Financial Software Systems (LSIS)

Because of the potential problems associated with large-scale integrated financial software systems, the regulatory agencies are issuing a joint policy statement to specifically identify the risks as well as management's responsibilities with respect to acquisition and/or development of such systems. The problems encountered by institutions include cost overruns, delays in implementation and internal control issues, as the attached statement indicates. In certain instances, financial institutions were able to implement only a portion of these systems or completely abandoned the project after considerable capital outlays. In view of the supervisory concerns, the agencies have agreed to alert institutions subject to their supervision to the risks associated with these systems.

Please distribute the enclosed document on large-scale integrated financial software systems to bank holding companies over \$1 billion and all State member banks in your district. Any questions regarding LSIS should be directed to Vince Provenzano (X3359) or Kathleen M. O'Keefe (X3412).

/s/James I. Garner
Assistant Director

Enclosure

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 88-37(FIS)
December 28, 1988

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

**SUBJECT: Disclosure of Numeric Composite Examination and Inspection Ratings to
Examined/Inspected Institutions**

On December 16, 1988, the Board approved a proposal, previously approved by the Conference of Presidents of the Federal Reserve Banks, for examiners to disclose the composite numeric rating assigned in an examination or inspection to the senior officials and boards of directors of examined/inspected institutions as part of the examination/inspection report process. Accordingly, effective immediately, composite numeric ratings assigned by examiners during examinations of state member banks, Edge Act and Agreement Corporations, overseas branches of U.S. banking organizations and inspections of bank holding companies are to be disclosed. Composite ratings that are assigned in the examination of trust activities, data processing, and compliance with the consumer laws and the Community Reinvestment Act are also to be disclosed to the appropriate officials of the examined institution.

The disclosure of the rating should be made in the summary sections of examination and inspection reports as well as in the summary reports prepared for boards of directors of examined/inspected institutions. In conjunction with disclosing the ratings, examiners and/or supervisory officials should explain clearly the meaning of the ratings. This will be of particular importance in the case of trust ratings, in that these ratings are assigned on a different scale than are commercial examination ratings. In addition, a rating should not be disclosed to an institution until it has been formally approved by appropriate senior Reserve Bank supervisory officials.

In disclosing the ratings, it should be made clear that they are part of the overall findings of an examination/inspection, and are confidential.

/s/William Taylor
Staff Director

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 89-16(FIS)
August 1, 1989

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: Interagency Policy on Contingency Planning for Financial Institutions

Enclosed is a copy of the Interagency Policy on Contingency Planning for Financial Institutions which is the result of an EDP Symposium conducted in September, 1988. In view of the increasing dependence on automated systems, it is imperative that financial institutions address the inherent risks associated with the loss or extended disruption of services. Accordingly, the primary purpose of this statement is to alert directors and management of financial institutions and service bureaus of the need for in-house contingency planning and also for the coordination of contingency planning between financial institutions and their service bureaus where applicable. It also addresses various issues and responsibilities relating to the development and implementation of such plans.

You are requested to distribute a copy of this policy to all bank holding companies, state member banks, Edge Act Corporations, and service bureaus in your District. Any questions regarding this policy should be directed to Vince Provenzano (202-452-3359).

/s/James I. Garner
Assistant Director

See FFIEC Policies SP-5 for details.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

**DIVISION OF BANKING
SUPERVISION AND REGULATION**

**SR 89-21(FIS)
September 26, 1989**

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: EDP Examination Data Base

Effective immediately, it is no longer necessary to prepare and forward a copy of the "Summary of EDP Evaluation" form for each EDP examination as required under the provisions of SR 83-16 (FIS), dated April 7, 1983. The FDIC has dispensed with requesting this form from the other federal banking agencies.

Questions or comments concerning the foregoing matter should be addressed to Vince Provenzano (202 452-3359).

/s/James I. Garner
Assistant Director

Supersedes: SR 83-16 (FIS)

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

**DIVISION OF BANKING
SUPERVISION AND REGULATION**

**SR 90-5
January 24, 1990**

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: Interagency Statement on EDP Service Contracts for Financial Institutions

Enclosed is a copy of the Interagency Statement on EDP Service Contracts for Financial Institutions. The intention of this issuance is to advise the financial community of the risks associated in contracting for EDP services and/or failing to properly account for certain contract provisions. Further, the Financial Institutions Reform, Recovery and Enforcement Act of 1989, among other things, prohibits FDIC insured depository institutions from entering into contracts if the performance of such contract would adversely affect the safety and soundness of the institution.

Please distribute this statement to all bank holding companies, state member banks, Edge Act Corporations and service bureaus in your district. Any questions regarding this policy should be directed to Vince Provenzano (202) 452-3359.

/s/James I. Garner
Assistant Director

See FFIEC Policies SP-6 for details.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

**DIVISION OF BANKING
SUPERVISION AND REGULATION**

**SR 91-21 (FIS)
October 11, 1991**

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: EDP Interagency Examination, Scheduling and Distribution Policy

Enclosed is a copy of the revised EDP Interagency Examination, Scheduling and Distribution Policy which was approved by the FFIEC Task Force on Supervision at their September 1991 meeting. This policy supersedes SR - 475, July 19, 1978; SR 492, October 11, 1978; and SR 79 - 549, June 4, 1979 and is effective immediately.

If you have any questions, please contact Vince Provenzano at 202-452-3359.

/s/James I. Garner
Assistant Director

Enclosure

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 93-25 (FIS)
May 14, 1993

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: Interagency Supervisory Statement on EFT Switches and Network Services

Enclosed is a copy of the Interagency Supervisory Statement on EFT Switches and Network Services which is the result of an FFIEC sponsored EDP Symposium. In view of the increased use of switch and network services to expand traditional methods of consumer banking, it is important that financial institutions address a number of concerns that arise in this context. As such, this statement was prepared to alert directors and management of financial institutions and service bureaus of the need for adequate controls, appropriate contractual arrangements and safe and sound settlement procedures.

The FFIEC issued a press release on April 7, 1993, indicating that the policy statement had been adopted. On April 8, 1993, "camera ready copy" of the press release was distributed to the president of each Federal Reserve Bank by the Board's Office of the Secretary. It was intended that the statement be distributed to all bank holding companies, state member banks, Edge Act Corporations, state licensed branches and agencies of foreign banks and automated data processing service bureaus in your District.

Any questions regarding this policy should be directed to Don Vinnedge (202-452-2717).

/s/ James I. Garner
Deputy Associate Director

ATTACHMENTS MAY BE OBTAINED FROM FEDERAL RESERVE BANK

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

**DIVISION OF BANKING
SUPERVISION AND REGULATION**

**SR 94-2 (FIS)
January 13, 1994**

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: Electronic Imaging Systems

The FFIEC's Task Force on Supervision recently approved for distribution to the agencies and their examiners the attached statement on "Control and Security Risks in Electronic Imaging Systems" which was prepared by the EDP Supervision Subcommittee following a symposium on the subject. The statement addresses risk and control issues inherent in a growing, highly technical speciality area that EDP examiners are encountering more frequently during examinations of banks and service centers.

Please distribute the statement to your EDP supervision staff and examiners in order to enhance their familiarity with the subject. The statement may be made available to banks and others upon request or where warranted. Should you have any questions regarding this statement, please contact Blaine Jones (202-452-3759).

/s/ Howard A. Amer
Assistant Director

See FFIEC Policies SP-10 for details.

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 95-7 (SPE)
February 9, 1995

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: Enhanced Supervision Program for Multiregional Data Processing Servicers

The attached policy statement on the "Enhanced Supervision Program for Multiregional Data Processing Servicers (MDPS)" was recently approved by the FFIEC's Task Force on Supervision in order to improve the agencies' understanding of the condition and operations of large EDP service centers between full-scope examinations. This program amends the existing "Interagency EDP Examination, Scheduling, and Report Distribution Policy Statement (SP-1)" which requires that the condition of MDPS vendors "...be monitored between examinations through periodic visitations and progress reports..."

In this regard, the attached statement is intended to formalize many of the agencies' interim monitoring practices and procedures that have evolved informally over the three years since the last revision to SP-1. It is also intended to provide for the uniform implementation of this requirement on an interagency basis.

The statement is effective immediately. Please distribute it to your EDP supervision staff and examiners. It may also be provided to MDPS organizations and others with an interest in EDP supervision policy. Should you or your staff have any questions, please contact Blaine Jones at the Board at (202) 452-3759.

/s/ Howard A. Amer
Assistant Director

Attachment

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 95-48 (SPE)
(Revised ¹)
November 9, 1995

TO THE FIRST VICE PRESIDENT AND OFFICER IN CHARGE
OF SUPERVISION AT EACH FEDERAL RESERVE BANK

SUBJECT: Fedwire Third-Party Access Policy

The Federal Reserve Board has approved certain modifications to its Fedwire Third-Party Access Policy (Policy) in order to clarify its applicability and to reduce the administrative burden on Fedwire participants attributable to several of its earlier provisions. These changes, which are described in the attached *Federal Register* notice, became effective August 10, 1995. Existing Fedwire third-party access arrangements are to comply with the revised policy by March 1, 1996.

Examination Procedures

Depository institutions that outsource either their Fedwire funds transfer or book-entry securities transfer operations may have to implement new operating procedures in order to comply with the requirements contained in the Policy. The revised Policy will also necessitate modifications to the System's existing examination procedures used by safety and soundness and EDP examiners to review electronic funds transfer and book-entry securities transfer operations. In this regard, supervision staff is currently reviewing the System's program for the examination of Fedwire operations.

Upon completion, the review will result in modifications to examination procedures that address the requirements of the Board's revised Policy. Until the revised examination procedures are finalized and approved for use, examiners assigned to review Fedwire operations at a bank that has outsourced any part of its operation to a third party should supplement existing procedures by making a special effort to focus attention on the outsourcing arrangement in order to determine that the bank is in compliance with the modified policy.

Examiners should pay particular attention to assess the bank's compliance with the policy's "termination back-up" requirement now applicable only in those cases where the Fedwire participant outsources to an **unaffiliated** third party. For a broader discussion of the issues pertaining to back-up requirements, see section F of the attached *Federal Register* notice.

¹ This letter revises the version issued on October 10, 1995, in order to clarify the review and approval process.

Review and Approval Process

The Policy is implemented through the Reserve Bank's funds transfer and book-entry securities transfer operating circulars, "Funds Transfers Through Fedwire" and "Book-Entry Securities Account Maintenance and Transfer Services," respectively. The Policy establishes conditions that must be met by domestic banks and U.S. branches and agencies of foreign banks that choose to outsource their Fedwire operations to a domestic service provider. Pending Board review of the issues pertaining to the use of a service provider located in a foreign country, the Federal Reserve will not authorize requests for foreign Fedwire third-party access arrangements, including those to foreign affiliates, branches or parent companies.

In accordance with the Policy, depository institutions that desire to outsource their Fedwire funds transfer or book-entry securities transfer operations to a domestic third-party service provider must receive approval from the Reserve Bank before establishing such an arrangement. In order to initiate this process, the depository institution (participant) must submit a request for a "Letter of Authorization" to its Reserve Bank. Such requests are ordinarily submitted to the Reserve Bank's operations staff. Reserve Banks are requested to establish appropriate internal review procedures for third-party access requests in order to ensure effective coordination between the operations and supervisory functions.

To date, most of the requests to establish Fedwire third-party access arrangements have been between affiliated parties. Pursuant to the modifications to the Policy that became effective August 10, 1995, Reserve Banks are now authorized to approve such requests without further review by Board staff. Given that the Policy is less restrictive for outsourcing arrangements to affiliates, the Reserve Bank need not require additional supporting documentation from the participant beyond its request form before approving the request. In effect, the participant's affirmations contained on the request form evidence its position that it has met the Policy's requirements. As part of the subsequent examination process, the participant's compliance with the Policy will be subject to review.

Board staff review of Fedwire outsourcing proposals continues to be a requirement in those cases where the participant is a subsidiary of a Top 50 bank holding company that proposes to outsource to an **unaffiliated** third-party service provider. In such cases, the Director of the Division of Reserve Bank Operations and Payment Systems (RBOPS) and the Director of the Division of Banking Supervision and Regulation (BS&R) must review the proposal and offer no objection before the proposal can be approved by the Reserve Bank. Such proposals should be submitted to the Director of RBOPS who will coordinate review with BS&R at the Board. Given the complexity of issues associated with outsourcing to unaffiliated third parties by large banking organizations, Reserve Banks should obtain from the participant more specific information concerning the participant's ability to comply with the Policy on an ongoing basis prior to recommending approval to Board staff. Special attention should be given to a review of the participant's plans to comply with the Policy's termination back-up requirement.

Comparably, Reserve Bank supervision staff should be actively involved, together with Reserve Bank operations staff, in the review of all proposals to outsource Fedwire operations to **unaffiliated** third parties, regardless of the size of the bank or its parent, to assess the participant's ability to comply with the Policy.

Distribution to Staff

Please distribute this SR letter and the attached *Federal Register* notice containing the Board's policy

statement to your supervision and operations staff, particularly those safety and soundness and EDP examiners that may be assigned responsibility for the examination of a bank's Fedwire operation and those staff that may be responsible for the review and analysis of Fedwire outsourcing proposals.

Should you or your staff have any questions regarding Fedwire supervisory matters, please contact Howard Amer, Assistant Director, BS&R, at extension 2958, or Don Vinnedge or Blaine Jones in the Trust/EDP Supervision Section at extension 2717 or 3759, respectively. Questions pertaining to Fedwire operations should be directed to Jeff Stehm or Lisa Hoskins in the Fedwire Section at extension 2217 or 3437, respectively.

/s/ James I. Garner

Deputy Associate Director
Division of Banking
Supervision and Regulation

/s/ Louise L. Roseman

Associate Director
Division of Reserve Bank Operations and
Payment Systems

Attachment:

Federal Register – Federal Reserve Payment
System Risk Policy

Cross Reference: Commercial Bank Examination Manual Section 4180
1994 FFIEC Information Systems Examination Handbook Section 8

TABLE OF CONTENTS

Number	Date	Subject
CUL-109	09-89	Information Processing Issues See FFIEC Policies SP-3, SP-4, and SP-5 for details.
CUL-122	02-91	Information Processing Issues See FFIEC Policies SP-6 and SP-7 for details.

National Credit Union Administration Board

CUL-109
September, 1989

**TO THE BOARD OF DIRECTORS OF THE FEDERALLY INSURED CREDIT UNION
ADDRESSED:**

INFORMATION PROCESSING ISSUES

For your reference I am enclosing papers from the Federal Financial Institutions Examination Council (FFIEC) which outline issues and risks associated with certain computer operations.

Credit unions will continue to benefit from "distributed" processing systems if proper controls are set up, as suggested in one of the papers. Likewise, large-scale integrated systems (LSIS) are becoming more common and also require proper controls, as indicated in another paper.

Guidelines for contingency planning are also included here. Each board of directors should ensure that a comprehensive contingency plan is put in place and tested regularly. Because such planning has become crucial to credit union operations, contingency plans and test results will be reviewed and evaluated during future supervisory examinations.

For the National Credit Union Administration Board,

/s/Roger W. Jepsen
Chairman

See FFIEC Policies SP-3, SP-4, and SP-5 for details.

National Credit Union Administration Board

CUL-122
February, 1991

**TO THE BOARD OF DIRECTORS OF THE FEDERALLY INSURED CREDIT UNION
ADDRESSED:**

INFORMATION PROCESSING ISSUES

For your reference, I am enclosing three papers, one from the National Credit Union Administration (NCUA) and two from the Federal Financial Institutions Examination Council (FFIEC), which outline issues related to the automated processing of credit union information.

Many credit unions use information system service bureaus for their data processing needs. There is the potential for certain risks to all financial institutions that contract out for these services. The first paper explains NCUA's program to examine and assess the safety and soundness of organizations that provide data processing services to federally insured credit unions. These reviews will bring NCUA in line with the other federal financial institution regulators that have been performing these types of examinations for many years.

On a related issue, the second paper alerts management to specific risks and accounting problems that have been identified in some federally insured financial institutions using data processing services from outside vendors.

NCUA continues to stress the importance of strategic planning in all areas of credit union operations. As such, I am releasing the third paper, addressing the issue of strategic information systems planning as part of the overall planning process for your institution.

For the National Credit Union Administration Board,

/s/Roger W. Jepsen
Chairman

See FFIEC Policies SP-6 and SP-7 for details.

ATTACHMENT

CUL-122

February, 1991

POLICY STATEMENT FOR THE REVIEW OF INFORMATION SYSTEM VENDORS:

The National Credit Union Administration (NCUA) has established a program to perform on-site examinations of information system vendors. This program was initiated because of the critical importance automated information systems have to many credit unions. There is the potential for a high degree of risk to credit unions and the National Credit Union Share Insurance Fund should problems occur with these vendors or their products. Assessing this potential risk, with both individual vendors and the industry as a whole, is a key element of this examination program.

BACKGROUND

Information system vendors provide a variety of products and services to federally insured credit unions. These include:

- service bureau services (remote, on-line information processing)
- turnkey systems (complete in-house information processing systems, including equipment and vendor developed and supported software)
- software products (for use on credit union-owned hardware)
- facilities management services (vendor supplied personnel and expertise to operate a credit union-owned system)

Vendors may be private companies or credit union service organizations (CUSOs).

SCOPE

NCUA will be accessing the overall safety and soundness of information system product providers. The following areas will, at a minimum, be included in the scope of our reviews:

- organization and management
- strategic planning
- financial condition
- data center controls
- systems and programming controls
- backup and recovery methods and testing
- contingency planning and testing
- customer contracts
- interest and dividend computations
- delinquency calculations

Other areas of a vendor's operation may be reviewed as necessary.

METHODOLOGY

NCUA will contract with third-party information system auditing specialists to act as our agents in performing these examinations. This is being done to augment our in-house information system auditing resources and facilitate the completion of work in a timely manner.

NCUA plans to perform reviews of approximately 20 information system vendors per year. Initially, we will focus on the largest service bureau vendors. In subsequent years, we will expand our reviews to include other information system providers and perform follow-up examinations as needed.

RESULTS

NCUA will work directly with information system vendors to correct any deficiencies found in our reviews. If deficiencies are corrected within a reasonable period of time, NCUA will not issue a report of our findings. If, however, a vendor will not agree to, or does not correct, any significant problems noted in our review, a written report of our findings will be issued to all credit union customers of the vendor and to all NCUA examiners.

(FILE NAME ON DISK # 2 = S3C29.WPD)

TABLE OF CONTENTS

Number	Date	Subject
BANKING/OCC BULLETINS		
OCC-94-8	01-27-94	Electronic Imaging Systems See FFIEC Policy SP-10 for details.
BANKING CIRCULARS		
BC 177 Revised	07-12-89	Corporate Contingency Planning See FFIEC Policy SP-5 for details.
BC 187	01-18-85	Financial Information on Data Processing Servicers
BC 203 Revised	04-30-87	Accounting for the Cost of Internally Developed or Purchased Computer Software
BC 226	01-25-88	End-User Computing See FFIEC Policy SP-3 for details.
BC 229	05-31-88	Information Security
BC 235	05-10-89	International Payments Systems Risks
BC 260	07-14-92	EDP Service Contracts See FFIEC Policy SP-6 for details.
BC 271	05-25-93	EFT Switches and Network Services See FFIEC Policy SP-9 for details.
EXAMINING CIRCULARS		
EC 238 Supplement 1	08-02-89	Specialty Rating Disclosure
EC-261	01-24-92	Interagency EDP Examination, Scheduling, and Report Distribution Policy See FFIEC Policy SP-1 for details.
OCC ADVISORY LETTERS		
AL-88-7	11-21-88	Large-Scale Integrated Financial Software Systems

See FFIEC Policy SP-4 for details.

AL-91-4

07-24-91

Social Security Numbers as Personal Identification Numbers

Comptroller of the Currency Administrator of National Banks

**OCC Bulletin 94-8
Date: January 27, 1994**

Subject: Electronic Imaging Systems

**To: Chief Executive Officers of all National Banks, Department and Division Heads, and
all Examining Personnel**

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

Examiners will use the attached paper as a guideline when reviewing the operations of departments using imaging systems.

For further information, contact the Office of the Chief National Bank Examiner, (202) 874-5170.

/s/ Donald G. Coonley
Chief National Bank Examiner

Comptroller of the Currency Administrator of National Banks

**Banking Circular 177
(Revised)
Date: July 12, 1989**

Subject: Corporate Contingency Planning

To: Members of the Board of Directors of all National Banks, Chief Executive Officers of all National Banks, Deputy Comptrollers, District Administrators, and All Examining Personnel

PURPOSE:

Attached is a joint policy statement by the Federal Financial Institutions Examination Council (FFIEC). This policy addresses the need for corporate-wide contingency planning by all financial institutions and their servicers. This includes developing strategies to minimize loss and to recover from significant disruptions in business operations. At a minimum, these strategies must address:

- centralized and decentralized operations,
- user department activities,
- communications systems (data and voice),
- bank functions linked to service bureaus, and
- recovery plans by the service bureaus.

The attached policy statement revises Banking Circular 177, dated April 16, 1987. However, it reflects no change in policy by this Office toward contingency planning for national banks. It does represent a uniform policy by the FFIEC toward this important issue.

ORIGINATING OFFICE

Bank Information Systems Policy Division, (202) 447-0468

/s/ Robert J. Herrmann
Senior Deputy Comptroller for Bank Supervision

See FFIEC Policies SP-5 for details.

Comptroller of the Currency Administrator of National Banks

Banking Circular 187
Date: January 18, 1985

Subject: Financial Information on Data Processing Servicers

**To: Chief Executive Officers of All National Banks, District Deputy Comptrollers
and all Examining Personnel**

PURPOSE

The purpose of this Banking Circular is to alert national banks to the importance of performing financial reviews of organizations providing data processing services and to set forth OCC policy regarding the subject.

BACKGROUND

Financial institutions have become increasingly dependent upon computers for daily operations and must assure themselves of continued, uninterrupted data processing support. Many institutions use external (independent) data processors to provide such support.

Due to financial problems, several data processing servicers have failed and others have weakened, to the extent that their ability to continue operations and/or provide dependable services is uncertain. In many instances, the serviced financial institutions were unaware of the servicer's financial problems, and as a result, were unprepared for the data center's failure or the data center's inability to provide an acceptable level of service.

DISCUSSION

Financial institutions can reduce the potential impact of a data center failure by being informed of the financial condition of their servicers. Once aware of financial problems or an inability to provide an acceptable level of service, a financial institution could engage in alternative servicing arrangements and avoid an interruption in its data processing support. An effective method of obtaining financial information is to require, in the contracts between financial institutions and servicers, that current financial information be submitted on a regular basis.

POLICY

A board of Directors or a committee thereof in order to satisfy its fiduciary responsibilities regarding data processing services would normally obtain and analyze the financial information of their data processing servicers on an annual basis. Audited, unconsolidated financial statements would facilitate the analysis. If a servicer's financial condition is deteriorating or unsound, alternative

servicing arrangements should be considered in order to assure continued data processing support. Prudent banking practices would normally include the documentation of such analysis/contingency plans. For more information on Contingency Planning for Electronic Data Processing Support, See Banking Circular #177.

ORIGINATING OFFICE

EDP Examinations Division, (202) 447-0468

/s/ John F. Downey
Chief National Bank Examiner

Comptroller of the Currency Administrator of National Banks

**Banking Circular
203
(Revised)
Date: April 30, 1987**

Subject: Accounting for the Cost of Internally Developed or Purchased Computer Software

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, Directors and Examining Personnel

PURPOSE

This issuance establishes a revised accounting policy for the cost of internally developed computer software consistent with generally accepted accounting principles.

REFERENCE

This Banking Circular supersedes the accounting policy previously established in Banking Circular No. 203, Accounting for the Cost of Internally Developed Computer Software. Banking Circular No. 203 is, therefore, rescinded.

POLICY

National banks should expense, as incurred, the cost of internally developed computer software developed for the bank's own use. This also includes the modification and implementation costs of purchased software.

Internally developed computer software which is intended to be sold, leased or otherwise marketed should be accounted for in accordance with Statement of Financial Accounting Standards No. 86 (FAS-86). "Accounting for the Costs of Computer Software to be Sold, Leased, or Otherwise Marketed." FAS-86 requires all such costs to be expensed as incurred until the software is determined to be technologically feasible. Thereafter, software production costs are to be capitalized and reported at the lower of unamortized cost or net realizable value. Amortization should be based on current and future revenues with the annual minimum amortization equal to the straightline amortization over the remaining estimated economic life of the product.

BACKGROUND

The Office of the Comptroller of the Currency (OCC) issued Banking Circular No. 203 because existing accounting literature provided only general guidance with respect to accounting for the cost of internally developed computer software. Further, this lack of specific guidance resulted in accounting policies which were not being consistently interpreted or applied.

Banking Circular No. 203 required all costs associated with internally developed computer software costs to be expensed as incurred. This policy applied both to software developed for the bank's own use, and to software intended to be sold, leased or otherwise marketed. When the Financial Accounting Standards Board later issued FAS-86, it varied with Banking Circular No. 203. This Circular revises the regulatory policy to be consistent with generally accepted accounting principles and FAS-86.

FAS-86 has excluded the costs incurred for an enterprise's development of computer software for its own use. This exclusion is based upon current accounting practice which heavily favors expensing such costs.

EFFECTIVE DATE

Costs incurred in the development of computer software for a bank's internal use must be expensed as of January 1, 1985. Retroactive application is encouraged.

Application of FAS-86 to costs incurred to develop computer software to be sold, leased or otherwise marketed is effective immediately. Retroactive application to the effective date set forth in FAS-86, fiscal years beginning after December 15, 1985, is allowed.

ORIGINATING OFFICE

Questions regarding this issuance may be directed to the Chief National Bank Examiner's Office. Bank Accounting Division (202) 447-0471.

/s/ William J. Stolte
Chief National Bank Examiner

Comptroller of the Currency Administrator of National Banks

**Banking Circular
226
Date: January 25,
1988**

Subject: End-User Computing

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators and All Examining Personnel

PURPOSE

Attached is a joint issuance by the Federal Financial Institutions Examination Council on risks associated with end-user computing activities. End-user computing represents information processing activities which utilize microcomputers, small mainframes, and/or other computer terminals, to control and process data at the user level. It is recognized as a necessary and important aspect of information processing and delivery for many financial institutions.

This issuance discusses some of the potential risks and possible controls which are appropriate for these activities. Supervision and controls, consistent with guidelines offered in this circular, are expected for each national bank utilizing end-user computer systems.

ORIGINATING OFFICE

EDP Activities Division, (202) 447-0468

/s/ Robert J Herrmann
Senior Deputy Comptroller
for Bank Supervision

Attachment

See FFIEC Policies SP-3 for details.

Comptroller of the Currency Administrator of National Banks

Banking Circular 229
Date: May 31, 1988

Subject: Information Security

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, and All Examining Personnel

PURPOSE

This circular alerts management of national banks to the importance of information security. It addresses the need to protect all types of information, particularly that which is produced, stored, and transmitted by computer.

BACKGROUND

Most bank information is created by or directly linked to computer processing. This includes customer records, financial transactions, business strategies, software systems, and even corporate correspondence. Financial data and business documents routinely are transmitted throughout a bank corporation via telecommunication lines linked to computers. Similar information also is transmitted outside the corporation, between the bank and its correspondents, its regulators, and its customers.

CONCERNS

Information, regardless of its source, is a valuable asset to the bank. Its accuracy and confidentiality is essential to the business. Accordingly, it must be protected from abuses such as inadvertent or intentional misuse, disclosure, fraud, and error. Information systems, both the data and the software that creates and stores the data, must be secure.

Data are created and stored in substantial volume, often representing millions of bank records and transactions. Correspondence and bank strategies also are created and stored through text processing. Bank and customer funds routinely are transferred via computerized payment networks. Transmission of these data regularly occur over public communications links, such as telephone lines and satellites. In addition, many users, including employees and bank customers, can directly access the data through computer terminals or telephones. Some have the ability to change information or create new data. These activities, while improving customer services and internal operations, also have increased the risk for error and abuse of the bank's information.

RECOMMENDATIONS

Controls must exist to minimize the vulnerability of all information and to provide necessary security. The level of control must be assessed against the degree of exposure and the impact of loss to the institution. This includes dollar loss, competitive disadvantage, damaged reputation, improper disclosure, lawsuit, or regulatory sanctions.

Various processes are available to strengthen information security in the banks. The most basic are sound written management policies for internal control. These include physical security, separation of duties, quality control, hardware and software access controls, and audit.

Information security controls should be designed to:

- ensure the integrity and accuracy of management information systems,
- prevent unauthorized alteration during data creation, transfer, and storage,
- maintain confidentiality,
- restrict physical access,
- authenticate user access,
- verify accuracy of processing during input and output,
- maintain backup and recovery capability,
- provide environmental protection against information damage or destruction.

Computer hardware and software technologies can help protect information resources. Although they vary, security features usually are available at each level of computer sophistication. Regardless of the controls adopted, they should apply to information produced and stored by both automated and manual methods.

The appendix to this issuance provides additional detail on some areas of risk and some technology controls. Additional control guidelines are detailed in the FFIEC EDP Examination Handbook.

POLICY

Information security is a functional responsibility. And as a means to protect assets, it must be a strategic objective of the business. A sound system of internal controls and management policies must be established and enforced to satisfy this objective.

The Board of Directors should require that information security policies exist throughout the bank corporation. These policies must be in writing and communicated to all personnel and other authorized users of bank information systems. Examiners may periodically target reviews of information security in the bank's supervisory strategy. These reviews may include:

- the adequacy of the "corporate information security policy,"
- compliance with the security standards, and
- management's supervision of these activities.

ORIGINATING OFFICE

Office of the Chief National Bank Examiner, Bank Information Systems Policy Division, (202) 447-0468

/s/ Donald G. Coonley
Chief National Bank Examiner
Attachment

BC-229 - Appendix

Banking Circular on Information Security

Some risk exists in every system and operation of the bank, whether manual or automated. Management must recognize the types of systems and operations that pose greater risks to information security. These might include:

- mainframe computer operations,
- microcomputer operations,
- communications networking,
- operating systems,
- applications software,
- end-user computing,
- distributed processing networks,
- system recovery activities,
- information retention and backup,
- text processing (office automation),
- document filing and retention,
- manual departmental operations.

Technology controls for information security might include:

Encryption

A process by which plain text is converted into encrypted strings of meaningless symbols and characters. This helps prevent unauthorized viewing and altering of electronic data transactions during transmission or storage. The Data Encryption Standard (DES) is commonly used for encoding PIN numbers on access cards, for storing user passwords, and for funds transfers on large dollar payment networks.

Message Authentication

A code (MAC) designed to protect against unauthorized alteration of electronic data transactions during transmission or storage. This code is used with data encryption to further secure transmission of large dollar payments.

Security Software

Application software designed to restrict access to computer-based data, files, programs, utilities, and system commands. Some systems can control access by user, by transaction, and by terminal. Security violations, including attempts can be reported. Access reports also can be produced.

Data Retention

The internal operations that require critical bank records to be regularly copied and stored in an offsite location. This includes data files, programs, operating systems, and related documentation. This also applies to critical data produced in hardcopy documents.

These are a few examples of controls and technologies to assist information security. New technologies and security methods are being developed and introduced constantly. The type and extent of controls must be measured against the degree of risk in any activity.

Comptroller of the Currency

Administrator of National Banks

Banking Circular 235

Date: May 10, 1989

Subject: International Payments Systems Risk

TO: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, and All Examining Personnel

PURPOSE

To alert national banks to the risks associated with large dollar payments systems, particularly within the international sector, Management is expected to adopt sound policies and supervisory practices for these activities. This office recognizes that these risks are more prevalent in larger banks. However, all national bank participating in payments systems, domestic and international, must assess these risks.

ISSUE

The worldwide exchange of financial transactions and information is expanding rapidly. An interlocking network of national and international markets, operating 24 hours a day, supports this activity. This network involves multiple payments, clearing, and settlement systems that handle trillions of dollars daily. In recent years, attention by bankers and regulators has focused on the operational, liquidity, and credit risks of large dollar payments systems. However, this attention mainly addressed national systems such as FEDWIRE and the Clearing House for Interbank Payments (CHIPS). International payments, clearing, and settlement systems also demand a high level of supervision and risk assessment.

Key to each system is the credit quality of its participants and its operational reliability. These vary widely among systems and countries. A weakness in either or both of these attributes can disrupt the system and possibly cause it to fail. This may occur if a creditor in a given system cannot settle, if the support systems cannot operate, or if there is sovereign intervention. A failure in one system could pose a liquidity problem for participants in that system. If the liquidity risk is not contained, for example, through government guarantees or some participant allocation, the crisis can become systemic. The crisis can spread rapidly from participating banks to nonparticipants because of the interlocks between systems and banks.

The underlying risks remain the same for both national and international systems. However, the limited ability to influence policies and controls in international markets increases the degree of risk to national banks.

POLICY

Management of each national bank is responsible for assessing risk in each payments, clearing, and settlement system in which the bank participates. Management must adopt adequate policies, procedures, and controls with respect to these activities. At a minimum, written policies should:

-
- Require periodic risk assessment of each system in which the bank participates;
 - Identify responsibility for assessing risks;
 - Document procedures to perform the assessments;
 - Require top management approval of participation in selected system;
 - Establish a process to monitor on-going payments systems risk;
 - Require written agreements between the bank and both its customers and the network; and
 - Include audit in the review and compliance with these policies.

Additional detail on the risks in settlement systems is included in the Appendix to this circular.

Originating Office: Bank Information Systems Policy Division (202) 447-0468

/s/ Robert J. Herrmann
Senior Deputy Comptroller for
Bank Supervision - Policy

BC-235 - Appendix

Banking Circular on International Payments Systems Risk

The risks in payment systems may be divided into three broad categories:

- credit (or counterparty) risks,
- sovereign risks, and
- operational risks.

The control processes to assess risk and monitor on-going activities must consider payment systems as a whole. Although individual risks exist, they are interrelated. The effect of a single event creates additional risks within the system. For example, the effect of a single participant failing to meet its credit obligation may cause the system not to settle. As such, credit and settlement risk are interrelated. In another example, an operational breakdown in the system or sovereign action disrupts payments flow. The system, in turn, does not settle and credit obligations are not met. This example involves operations, settlement, and credit risk within the system.

Senior management must be both aware of and able to monitor exposure. Operating units of some banks are located throughout the world and may be participating in a number of payments systems. To control risk in these situations, some degree of centralized review is needed. This is particularly important in banks where local business units have significant autonomy. These banks may rely on local management to assess and manage the risks of participating in a network. Therefore, a bank's interdependency between systems also must be considered.

The control banks can exert over the systems in which they participate often is limited. A bank normally does not own or operate the systems. Bank management therefore must establish a process that assists them:

- Understanding the risks posed by participation in payment systems;
- Identifying bank policies designed to manage these risks; and
- Implementing procedures and operational controls to manage risk.

The following briefly identifies several control issues, types of settlement systems, and associated risks. These are not all encompassing. Much more detail is needed to perform a comprehensive risk assessment on any settlement system.

Other references include two recently published reports on this issue.

- 1) Report on Netting Schemes - February 1989
- prepared by the Group of Experts on Payment Systems of the Central Banks of the Group of Ten Countries
- 2) Clearance and Settlement Systems in the World's Securities Markets - March 1989
- prepared by the Group of Thirty

International Payments Systems Risk Appendix

CONTROL ISSUES

Management need to consider and resolve numerous issues when participating in payment systems. These issues are generally the same for both national and international systems.

Guidelines should consider:

- Controls to reduce sender and receiver risks. These should include:
 - Bilateral credit limits,
 - Debit cap limits, including the process to determine these limits.
 - A process to monitor and control these limits on a real time basis.
- Controls to limit the overall exposure of the system, including debit cap limits.
- Requirements of the system to ensure that settlement occurs. This should address:
 - conditions for settlement such as the location, time, and settling procedures.
 - the type of settlement (i.e., provisionality or finality of payment).
 - the guarantor(s), if any, of payment finality. This may involve a central bank, the system owner/operator, and/or the system participants.
 - the basis for providing necessary liquidity to the system. This may require allocation of funding by participants, coinsurance, or central bank guarantees.
- Legal issues governing the system operation, including local laws, business practices, and government regulation.
- The capabilities of the system and the bank to handle emergency situations. This may require backup operations or the ability for the bank to bypass the network.
- Responsibility for reviewing the bank's participation in payment systems.

SETTLEMENT SYSTEMS

NET SETTLEMENT SYSTEMS

Net settlement are systems in which transactions accumulate during a processing day. Transactions are posted to participant accounts on a provisional basis until final settlement. At end of the day, net debit positions pay, net credit positions settle, and all transactions become final. CHIPS is this type of system.

MATCHED SETTLEMENT SYSTEMS

Matched settlement systems are systems in which each transaction is "matched" by comparing messages from both counter parties to the transaction. Only exactly matched messages are allowed to enter the system to form a transaction. At the end of the processing day, the matched transactions become the basis for payment instructions issued to participants' clearing banks. Once payment is made, a transaction becomes final. CEDEL is this type of system.

International Payments
Systems Risk
Appendix
Page 3

GUARANTEE SETTLEMENT SYSTEMS

Guarantee settlement systems are systems in which payment finality is guaranteed by a central bank. Because payments are irrevocable, they eliminate risk to the receiver of funds. There is no credit risk to participants in such a system. However, the sovereign and operational risks may remain. A good example of this type of system is FEDWIRE, in which the Federal Reserve guarantees payment and finality. That system is still subject to potential risks from government action or operational failure.

SYSTEM RISKS

CREDIT RISKS

Sender Risk

Sender risk is the risk that a depository assumes when it makes an irrevocable payment on behalf of the customer through an extension of credit. Credit can be extended explicitly, by granting a loan, or implicitly, by paying against uncollected or provisional funds or against insufficient balances.

Receiver Risk

Receiver risk involves risk to an institution upon acceptance of funds from the sender. This may be a customer, another institution, or the payments system. As the receiver of funds, an institution must rely on the sender's ability to settle its obligations at the end of day. Receiver risk is present when payments are revocable within the system until final settlement.

SETTLEMENT RISKS

Settlement risk is the risk that each participant in the system will be able to honor all obligations at time of settlement. If one participant fails to settle, this may disrupt settlement for other participants. As a result, the system's settlement fails. This also is referred to as liquidity risk. Like receiver risk, settlement risk is present when payments are conditional or revocable until final settlement. Settlement risk also is an exposure subject to operational disruptions or sovereign actions.

NET SETTLEMENT SYSTEM RISKS

Net settlement systems bear all the risks identified above. However, an additional risk is that of default by the system itself. The system serves as a clearing mechanism for all transactions. At settlement, it posts a net debit or credit position to each participant's account. Each participant in a net debit position must provide funds to settle its position. If unable to settle, the system must cover the shortfall. If not, netted transactions unwind and other participants are affected.

International Payments
Systems Risk
Appendix
Page 4

The financial strength of the net settlement system itself, therefore, is a significant factor to assess. Often, this is provided through member pro rata guarantees or allocations. Also, the system's membership standards and operating procedures should ensure that the creditworthiness or operating practices of its members do not endanger the functioning of the system.

MATCHED SETTLEMENT SYSTEM RISKS

Credit risk in a matched settlement system should be addressed in the same way as for any bank customer. In matched systems the counterparty in a transaction is known to the bank and exposure to any one counterparty may be monitored and controlled through establishment of credit limits.

However, even in matched settlement systems attention should be given to the system's membership standards and operating procedures. The default of a participant may still impact a bank which has no settlements outstanding with it by the effect of the default on other participants with whom a bank does have understanding settlements.

SYSTEMIC RISKS

Systemic risk is an outgrowth of settlement risk. The failure of one participant to settle deprives other institutions of expected funds and prevents those institutions from settling in turn. To the extent that chains of obligations develop, it is possible for a participant doing no business at all with a failed institution to suffer because of the effect of the failed institution on an intermediate participant and its ability to settle.

LEGAL RISKS

Any transaction occurring in a payments system is subject to the interpretation of courts in different countries and legal systems. This issue is normally addressed by the adoption of "governing law" provisions in the rules of the systems themselves. These provide for all disputes between members to be settled under the laws of a specific jurisdiction. However, they may be of limited value if a local court refuses to recognize the jurisdiction of a foreign court. This risk is difficult to address because there is no binding system of international commercial law for electronic payments. Banks should seek legal opinions regarding the enforceability of transactions settled through a particular system.

SOVEREIGN RISKS

Sovereign risk applies to all types of payments systems. It is the risk that action by a government may affect either a system or particular participants in a system. This action could be detrimental to other participants in the system. An example of this risk would be the imposition of exchange control regulations on a bank participating in international foreign exchange activities. While the bank itself may be both willing and able to settle its positions, government intervention prevents it from doing so. This risk can be controlled by monitoring a bank's exposure to counter parties located in nations where this type of action is considered possible.

**International Payments
Systems Risk
Appendix
Page 5**

OPERATIONAL RISKS

Operational risks include:

- a) system failure - caused by a breakdown in the hardware and/or software supporting the system. This may result from design defects, insufficient system capacity to handle transaction volumes, or mechanical breakdown, including telecommunications.
- b) system disruption - the system is unavailable to process transaction. This may be caused by system failure, destruction of the facility (natural disasters, fires, terrorism) or operation shutdown (employee actions, business failure, or government action).
- c) system compromise - resulting from fraud, malicious damage to data, or error.

The loss of availability of the payment system from whatever source can adversely affect major participants, their correspondents, markets, and interdependent networks.

Operational risks should be controlled by the banks through a sound system of internal controls including physical security, data security, systems testing, segregation of duties, backup systems, and contingency planning. In addition, a comprehensive audit program to assess risks, adequacy of controls, and compliance with bank policies is essential.

Since most banks are third party participants in international networks, their ability to influence controls is limited. Nevertheless, they must recognize risks to their own business operations and compensate through their own internal controls. In addition, banks should exercise their influence over third party systems to the extent possible to insist upon sound operations for system continuity and integrity.

Comptroller of the Currency Administrator of National Banks

**Banking Circular 260
Date: July 14, 1992**

Subject: EDP Service Contracts

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, Department and Division Heads, and all Examining Personnel

BACKGROUND

This issuance replaces BB 90-4 dated February 16, 1990. The FFIEC statement is unchanged.

SUMMARY

Attached is an "Interagency Statement on EDP Service Contracts" issued by the Federal Financial Institutions Examinations Council (FFIEC). This statement alerts financial institutions to potential risks in contracting for EDP services and failing to properly account for certain contract provisions.

Management of national banks is cautioned against contracting for services that include excessive fees or "inducement" provisions similar to those described in this statement. Furthermore, accounting for transactions under the contracts must conform to generally accepted accounting principles and call report instructions. This office considers contracting for excessive servicing fees, or failing to properly account for such transactions, an unsafe and unsound banking practice.

ORIGINATING OFFICE

Office of the Chief National Bank Examiner (202) 874-5170

/s/ Donald G. Coonley
Chief National Bank Examiner

See FFIEC Policies SP-6 for details.

Comptroller of the Currency Administrator of National Banks

Banking Circular 271
Date: May 25, 1993

Subject: EFT Switches and Network Services

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, Department and Division Heads, and all Examining Personnel

PURPOSE

Attached is a joint statement by the Federal Financial Institutions Examination Council on risks associated with retail electronic funds transfer (EFT) switches and associated network services. EFT switches allow customer-initiated transactions to accounts through another institution's terminals, such as ATM or point-of-sale devices. The statement does not address wholesale or large dollar transfer systems.

The statement discusses some potential risks of such activities and possible ways to control them, both in the users' and the providers' operations. Each national bank EFT switch user and its processor are expected to maintain supervision and controls consistent with the guidelines in the statement.

POLICY

Examiners will schedule examinations of EFT switch and network service providers the same as for any other provider of data processing services to national banks. They will rely on applicable portions of the FFIEC EDP examination work program and the attached statement for procedures.

ORIGINATING OFFICE

Office of the Chief National Bank Examiner, (202) 874-5170

/s/Donald G. Coonley
Chief National Bank Examiner

See FFIEC Policies SP-9 for details.

Comptroller of the Currency Administrator of National Banks

**Examining Circular 238
Supplement 1
Date: August 2, 1989**

Subject: Specialty Rating Disclosure

**To: Deputy Comptrollers, District Administrators, Department and Division Heads
and All Examining Personnel**

PURPOSE

This supplement informs all examining personnel of a change in OCC policy regarding disclosure of trust, EDP, consumer compliance and Community Reinvestment Act (CRA) ratings to banks.

BACKGROUND

The OCC assigns ratings under uniform interagency rating systems for trust, data processing operations, consumer compliance and the Community Reinvestment Act. The trust, consumer compliance, and CRA ratings have not previously been disclosed to individual national banks. The EDP rating currently is not being disclosed to data centers.

POLICY

Effective immediately, the composite trust, consumer compliance and CRA ratings will be disclosed, in writing, to national banks (e.g., in the supervisory letter). The ratings will be assigned by the office that supervises the bank. Examiners should not disclose the ratings to the bank because recommended ratings are not final until approved by the supervisory office. Further, the examiner should not discuss the ratings with the bank; the ratings are not subject to negotiation. Individual component ratings should not be disclosed.

Composite ratings for data processing operations will be disclosed in writing to the bank or center examined. EDP ratings should not be disclosed to customers of the vendor. The ratings will be assigned by the office that supervises the data center. The examiner should not discuss the ratings with the data center. Individual component ratings should not be disclosed. This issuance does not change the report and distribution procedures established by Banking Circular 109 and Supplement 1 to that circular, which remain in effect.

The written communication should refer to the ratings definitions. The definitions may be included in the appendix to the ROSA or on a supplemental paper. Alternatively, the communication may refer to an external source (e.g., "see the FFIEC's EDP Examination Handbook, Section 14.3 for further information," or "see the Comptroller's Handbook for Consumer Examinations, Section 504.500 and 504.500 for further information").

Composite ratings assigned before the effective date of this supplement should not be disclosed. Ratings should be disclosed only going forward, as they are assigned, confirmed or changed. The supervisory office will decide when and how to inform the bank or data center of its ratings. Written communication should be made within a reasonable period after the rating is assigned.

The bank or data center should be cautioned that it may not disclose the ratings. Disclosure of the trust, EDP, consumer compliance, or CRA ratings by the bank's director, officers, etc., will be considered a violation of 12 C.F.R. 4.18 (c) and subject to penalties in 18 U.S.C. 641, as is disclosure of the contents of the Report of Supervisory Activity.

ORIGINATING OFFICE

Consumer Activities Division (202) 874 - 5190

/s/ Robert J. Herrmann
Senior Deputy Comptroller for Bank Supervision Policy

Comptroller of the Currency Administrator of National Banks

Examining Circular 261
Date: January 24, 1992

Subject: Interagency EDP Examination, Scheduling, and Report Distribution Policy

**To: Deputy Comptrollers, District Administrators, Department and Division Heads,
and all Examining Personnel**

PURPOSE:

Attached is a joint policy statement by the Federal Financial Institutions Examination Council (FFIEC). This policy updates procedures for joint or rotated examinations of data centers providing services to insured financial institutions supervised by more than one federal regulatory agency. It also provides policy for the administration of the Multiregional Data Processing Servicer (MDPS) program.

The attached policy statement replaces BC-109, dated May 31, 1978, and its supplement. It reflects only minor changes, except those concerning distribution of reports and, for MDPS, examination scheduling.

ORIGINATING OFFICE:

Office of the Chief National Bank Examiner, (202) 874-5170.

/s/Donald G. Coonley
Chief National Bank Examiner

See FFIEC Policies SP-1 for details.

Comptroller of the Currency Administrator of National Banks

Advisory Letter 88-7
Date: November 21, 1988

Subject: Large-Scale Integrated Financial Software Systems

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators and All Examining Personnel

PURPOSE

Attached is a joint issuance by the Federal Financial Institutions Examination Council. The paper discusses advantages and disadvantages associated with large-scale integrated financial software systems (LSIS). It alerts financial institutions to the potential risks and controls appropriate for the development, implementation and use of these systems.

LSIS systems are software products which combine several banking applications in one package. They are becoming more common, particularly among larger banks, as a means of improving the institution's competitive position and information systems. Bank executives and directors should be aware of and concerned about the potential problems with these systems. Banks using or considering LSIS should implement applicable supervision and controls, consistent with guidelines in this paper.

ORIGINATING OFFICE

EDP Activities Division

/s/Robert J. Herrmann
Senior Deputy Comptroller for Bank Supervision Policy

See FFIEC Policies SP-4 for details.

Comptroller of the Currency Administrator of National Banks

**Advisory Letter: 91-4
Date: July 24, 1991**

Subject: Social Security Numbers As Personal Identification Numbers

**To: The Chief Executive Officer and the Compliance Officer of Each National Bank
and all Examining Personnel.**

The purpose of this advisory is to alert you to the potential for security breaches or fraud through unauthorized access to customer accounts.

We are aware that some banks are allowing their customers to use the telephone to access account information and transfer funds between accounts. In many cases the customer only has to key in the account number and the last four digits of his or her social security number, which serves as the personal identification number (PIN). The use of the customer's social security number, or any other commonly used number, as the PIN, could make unauthorized access to customer accounts or frauds easier.

Social security numbers are now used in many states for driver license numbers or are required on the license. Many merchants who cash personal checks or accept payment by check require the customer's driver license number for identification purposes. As a result, anyone in possession of this information could access a customer's account.

We recommend that banks that offer telephone access to customer accounts devise PIN numbers that ensure adequate security for customer accounts. The use of social security numbers for PIN numbers may not safeguard account security for bank customers and could subject the bank to civil liability. In addition, national bank examiners may cite this practice as an internal control exception.

If you have any questions about this advisory please contact your supervisory office or the Compliance Management Department at (202) 874-4810.

/s/Phillip R. Freer, Jr.
Acting Deputy Comptroller for Compliance Management

TABLE OF CONTENTS

Number	Date	Subject
RB 21	11-22-89	Servicing Contracts
TB 11	12-09-88	Interagency Supervisory Policy on Large Scale Integrated Software Systems (LSIS) See FFIEC Policy SP-4 for details.
TB 11-1	04-20-89	Purchased Software Evaluation Guidelines
TB 29	03-22-88	End-User Computing See FFIEC Policy SP-3 for details.
TB 30	07-13-89	Contingency Planning Interagency Policy on Contingency Planning for Financial See FFIEC Policy SP-5 for details.
TB 44	02-07-90	Interagency Statement on EDP Service Contracts See FFIEC Policy SP-6 for details.
TB 46	05-01-90	Contracting for Data Processing Services or Systems
TB 59	04-07-93	Interagency Supervisory Statement on EFT Switches and Network Services See FFIEC Policy SP-9 for details.

Office of Thrift Supervision

Regulatory Bulletin 21

Servicing Contracts

November 22, 1989

Summary:

To notify the District examinations staff of the need to review contracts for EDP and other vital services during safety and soundness/compliance examinations.

For Further Information Contact:

The Office of Thrift Supervision for the District in which you are located or the Division of Compliance Programs, Office of Thrift Supervision, Washington, D.C.

Background

Recently, financial institutions (banks, thrifts, credit unions) have been entering into fixed-priced, long-term servicing contracts which could ultimately have an adverse effect on the institution. In some instances service bureaus have offered certain inducements to the institutions as an incentive to convert to the service bureau. Examples of these inducements include offers:

- To purchase the institution's existing data processing equipment at book value, which substantially exceeds its current market value;
- To purchase other assets from the institution (e.g., real estate owned) at book value, which may exceed current market value;
- To provide capital by purchasing stock from the institution;
- To provide "cash advances" to the institution once the conversion process is complete; and
- To defer expense recognition of conversion costs or processing fees under the terms of lease or licensing contracts.

Generally, these inducements represent an attempt by the institution to maintain capital by deferring losses on the disposition of assets or avoiding expense recognition for current charges. As such, the institution's treatment typically is inconsistent with generally accepted accounting principles (GAAP) and the OTS quarterly report instructions.

Until recently, EDP servicing contracts usually have been written based on a pricing structure tied to the number of accounts and items processed. Contract terms were normally one to three years in length and provided reasonable means for cancellation. Some contracts are now being written with terms of up to ten years in length which are based on a fixed price, regardless of volume. These contracts usually provide for a significant increase in costs after the first few years and contain substantial cancellation penalties, especially if the original proposal involved the purchase of equipment and/or the transfer of personnel from the institution to the service bureau. Additionally, if the institution is unable to increase volume in proportion to the increase in annual service fees, the fees may become a substantial drain on the earnings of the institution.

Examiners should pay particular attention to these contracts to insure that the institutions have not entered into agreements with severe penalties that make switching to another service bureau or back

to in-house processing a non-viable alternative, even at the expiration of the contract.

Examiners should also assure themselves that the service bureau is providing for a level of service that meets both the present and the long-term needs of the institution. With the rapid changes occurring in EDP technology, it would appear difficult to project the EDP needs of any institution for a ten-year period.

Examination Considerations

Examiners should review all arrangements between a provider of vital services and the institution. The review should include the servicer's proposal and contracts. A determination should be made as to the extent to which the institution obtained proposals from other servicers and the evaluation process the institution utilized in making its selection. The examiner should be aware that frequently the servicer's proposal to the institution will stress advantages that the institution will realize from the contract while not mentioning any disadvantages. In many instances, the institution is focusing on short-term benefits and does not fully weigh the long-term costs of the contracts.

Examiners are especially reminded to scrutinize any loan or other transaction involving the servicer. This includes loans to the servicer which are written at unusually favorable terms, such as non-interest bearing loans and loans which are not enforceable if the contract is terminated or the institution is closed by regulatory authorities. The examiner also should review any significant deposit accounts maintained by the servicer. Any transaction involving the transfer of assets of questionable value from the institution to the servicer at an inflated value (usually book value) also should be investigated.

While many areas that the examiner should be aware of have been indicated, these are only guidelines. The vehicle employed by the servicer and institution may vary from case-to-case. However, the one consistent factor in these transactions is that they are favorable to the servicer, but may not be in the overall best interest of the institution.

Financial Institutions Reform, Recovery, And Enforcement Act of 1989 (FIRREA) Implications

Section 225 of FIRREA amends the Federal Deposit Insurance Act (FDIA), adding Section 30 which includes the following provision:

- (a) In General. An insured depository institution may not enter into a written or oral contract with any person to provide goods, products, or services to or for the benefit of such depository institution if the performance of such contract would adversely affect the safety or soundness of the institution.

Action to enforce compliance with this section may be taken under Section 8 of FDIA, and may include a requirement that the depository institution properly reflect the transaction on its books. Section 8 of FDIA provides the Federal banking agencies with the authority to issue cease-and-desist orders to ensure that depository institutions discontinue unsafe and unsound operating practices. Section 902 of FIRREA expands the authority of FDIA to include savings association affiliates and entities.

/s/Jonathan L. Fiechter
Senior Deputy Director Supervision Policy

Office of Thrift Supervision

Thrift Bulletin 11

Large Scale Integrated Software System (LSIS) Control Guidelines

December 9, 1988

Summary:

The purpose of this policy statement is to alert financial institutions to the risks associated with these sophisticated software systems and to identify the responsibilities of management when acquiring, developing, and using such systems. Management in each insured institution utilizing Large Scale Integrated Financial Software Systems should implement controls consistent with guidelines in this Bulletin.

For Further Information Contact:

The FHLBank District in which you are located or the Compliance Programs Division of the Office of Regulatory Activities, Federal Home Loan Bank System, Washington, DC.

/s/Darrel W. Dochow
Executive Director

See FFIEC Policies SP-4 for details.

Office of Thrift Supervision

Thrift Bulletin 11-1

Purchased Software Evaluation Guidelines

April 20, 1988

Summary:

This Bulletin alerts the board of directors and management of thrift institutions to potential risks and control issues in purchasing vendor software. It provides general guidelines for evaluating vendor software packages prior to their acquisition.

For Further Information Contact:

The FHLBank District in which you are located or the Compliance Programs Division of the Office of Regulatory Activities, Federal Home Loan Bank System, Washington, DC.

Background/Concerns

In recent years, there has been an increase in the number of companies developing and marketing software systems to meet the data processing and information needs of the thrift industry. Software packages can be obtained from a variety of sources such as large EDP system manufactures, software vendors, and accounting firms.

There are potential risks and control issues that should be addressed when institutions consider the purchase of software systems. Some institutions have found that software does not work as expected, is not adequately supported by the vendor, or requires costly changes in existing data processing systems that were not identified prior to purchasing the software. These situations can occur if the institution lacks management guidelines for evaluating software packages or if it does not have the expertise to perform these evaluations.

For example, poorly defined user requirements may result in the selection of software that does not meet the needs of the institution, or a weak cost-benefits analysis may not identify all direct and indirect costs of installing a software package. In other cases, an ineffective financial analysis may fail to evaluate the capability of the company to support the software after installation. As a result of these and other weaknesses, institutions can incur significant costs for software or hardware modifications that were not considered or brought to light in the evaluation process. In some instances, institutions have elected not to implement newly purchased software, resulting in a monetary loss to the institution.

Policy

The board of directors and management are responsible for ensuring that policies and procedures are in place and that resources are available to properly evaluate the risks and control issues of purchased software and vendor companies prior to purchase.

Guidelines

The following guidelines are provided to assist the board of directors and management in evaluating software packages and vendor companies prior to purchasing software. They are recommended for significant software purchases or when the software will support critical aspects of the institution's operations. These guidelines identify the type of studies or analyses that should generally be performed to improve the evaluation process and reduce the risk of the software not meeting the needs of the institution. In cases where there are limited alternatives for purchasing software such as single vendor applications, or operating system software designed for selected manufacturer's hardware, portions of the guidelines may not be applicable.

User Requirements Analysis

It is generally appropriate to analyze user requirements before evaluating vendor software packages. This analysis should usually define the business reason for purchasing software, deficiencies of the current system, user and data processing requirements, user and management reporting requirements, system interfaces to other systems, and the in-house resources needed to install and maintain the system. User, Data Processing, and the Audit Departments should generally be involved in this analysis. The resulting document will provide a basis for evaluating vendor software packages.

Cost-Benefit Study

After the user requirements analysis is completed, the direct and indirect costs of installing and maintaining purchased software should be compared to other business alternatives such as the use of service bureaus, modifications to existing applications, or manual systems. The capabilities and costs of each alternative should be analyzed and compared in a common format. The purchased software alternative should include the costs of modifications to existing data processing systems and expected return on investment.

If the results of the user requirements analysis and cost-benefit study indicate purchased software is cost-effective and the preferred solution, the following factors should be evaluated.

Financial Stability of the Company

The financial statements and resources of the software company should be analyzed to determine if the company is financially sound and has the resources to support and maintain the software package during its estimated life span. This analysis is especially important if the vendor is responsible for future modifications to the software programs. In these cases, procedures should be established to analyze the financial statements, performance, and stability of the company on an annual basis.

Contract Review

The software company's contract should be carefully reviewed by appropriate management and legal personnel to identify potential risks for the institution. This review should identify the contract deliverables, scheduled delivery dates, method of delivery, documentation, and other key contract terms. It should also include the obligations of the software company to support the software after purchase, furnish updates, and arrange for supplying the program source code and documentation if the software company goes out of business. The provisions for terminating or extending the contract should be clearly spelled out. Recourse for monetary losses as a direct result of errors in the software should also be considered. Requirements for annual financial information, preferably audited, should be incorporated into the contract.

Institutions making a substantial investment in new software should consider including in the contract the right of internal audit staff and FHLB examiners to perform examinations of the software companies for risk and control issues relating to the software purchase.

User References

User references are an important source of information in evaluating vendor packages. A user reference list of other institutions using the software package should be obtained from the vendor. These companies should be contacted to obtain information such as the software package purchased, the computer system used to run the software, modifications that were made after installation, the length of time in use, the quality of vendor conversion support, performance on similar hardware, and other pertinent information.

On-site visits to other institutions that have installed the software on a similar computer system should be considered before making a substantial investment in a software package. Care should also be taken in purchasing software that has not been installed and thoroughly tested in other locations.

Audit and Security Considerations

The software package should be reviewed for security controls and audit trails such as access to data files, authorizations, password controls, data access logs, reporting of security violations, and capabilities of utility programs to alter data.

Life Span of the Product

The age of the software, the number of updates issued since it was developed, the software vendor's plans for future modifications, and the useful life of the package should be evaluated against the institution's short-and long-term business plans.

Documentation

The documentation and manuals provided with the software package, and on-line help programs if the system is interactive, should be carefully reviewed by Data Processing and User Departments for content, readability, and completeness. This review should include input forms and output reports, compliance with in-house standards, and documentation provided with modifications.

Testing

Vendors should test all parts of the system in a systematic manner. Information on the testing procedures performed by the vendor should be obtained and evaluated. This information should include test plans, the hardware used for testing, and the method used to verify that the software calculations meet regulatory requirements, e.g., Truth In Lending disclosure calculations.

Conversion Assistance

The background and experience level of software company personnel assisting the institution in conversion planning, support, and training activities should be obtained and evaluated. The vendor should provide a detailed schedule of pre- and post-conversion support activities with associated costs. Conversion support materials should be carefully reviewed for quality, readability and completeness. The software company internal resources required to support conversion training should also be evaluated. The quality of conversion support provided by the vendor should be verified when checking user references.

Maintenance Support

The capability of the vendor company to provide timely, on-going maintenance support for user

programming requests, product updates and regulatory changes should be evaluated. The content, frequency and costs of previously issued software updates should be reviewed. The software should also be evaluated for report-writing capabilities that permit in-house personnel to produce new or specialized reports for management, user departments, or to comply with regulatory requirements. If vendor programming is required for report modifications, these costs should be considered in the evaluation.

Software Installation

After evaluation and selection of a software package that meets the needs of the institution, the software contract should be approved by senior management. Management should provide for an effective project control system to facilitate planning and implementation of the software. Liaison personnel should also be designated to manage the vendor relationship and coordinate the software installation.

/s/Darrel W. Dochow
Executive Director

Office of Thrift Supervision

Thrift Bulletin 29

End-User Computing

July 10, 1989

Summary:

This Bulletin supersedes R67-1 which is hereby rescinded. The contents have not changed. This Bulletin is meant to provide guidance to management for evaluating potential risks, and for implementing adequate control practices and responsibilities in end-user computing environments. It is expected that management in each insured institution utilizing end-user computer systems will implement controls consistent with guidelines offered in this Bulletin.

For Further Information Contact:

The FHLBank District in which you are located or the Compliance Programs Division of the Office of Regulatory Activities, Federal Home Loan Bank System, Washington, DC.

/s/Darrel W. Dochow
Executive Director

See FFIEC Policies SP-3 for details.

Office of Thrift Supervision

Thrift Bulletin 30

Interagency Policy on Contingency Planning for Financial Institutions

July 19, 1989

Summary:

This Bulletin supersedes R 67 which is hereby rescinded. It updates R 67 to require institution-wide contingency planning as opposed to focusing on centralized computer operations. It is expected that management of each financial institution will implement policies consistent with this Bulletin.

For Further Information Contact:

The FHLBank District in which you are located or the Compliance Programs Division of the Office of Regulatory Activities, Federal Home Loan Bank System, Washington, DC.

/s/Darrel W. Dochow
Executive Director

See FFIEC Policies SP-5 for details.

Office of Thrift Supervision

Thrift Bulletin 44

Interagency Statement on EDP Service Contracts

February 7, 1990

Summary:

The Office of Thrift Supervision, Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and the National Credit Union Administration have jointly issued the attached interagency statement on EDP Service Contracts to all federally supervised financial institutions. The statement alerts financial institutions to potential risks in contracting for EDP services and/or failing to properly account for certain contract provisions.

For Further Information Contact:

Your District office or the Division of Compliance Programs, Office of Thrift Supervision, Washington, D.C.

/s/Jonathan L. Fiechter
Senior Deputy Director
Supervision Policy

See FFIEC Policies SP-6 for details

Office of Thrift Supervision
Thrift Bulletin 46
Contracting for Data Processing Services or Systems

May 1, 1990

Summary:

This Bulletin supersedes R-13a which is hereby rescinded. This Bulletin has been amended to reference the pertinent sections of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA). A provision also has been added recommending that an institution's legal counsel review EDP contracts prior to ratification. Finally, a provision has been added relating to contracting for EDP services, under which EDP vendors agree to submit to examination by the Office of Thrift Supervision (OTS).

For Further Information Contact:

Your District office or Compliance Programs, Office of Thrift Supervision, Washington, D.C.

Background

Data processing activities have become essential to the efficient delivery of customer services and to the operation of most thrift institutions. Recent trends indicate that thrift institutions are finding data processing service organizations to be a cost effective alternative for many of their data processing needs rather than relying solely on in-house computer systems.

The provision of EDP services to financial institutions by service organizations entails certain risks and responsibilities. Contracts for EDP services and systems should appropriately define and balance those risks and responsibilities between the vendor and the institution.

Policy

Thrift institution management should carefully review any proposed data processing service contracts or agreements to minimize the institution's exposure to risk, and should follow the guidelines listed below prior to signing any contracts with vendors of EDP services. Furthermore, the institution's legal counsel should review the draft contract to determine that the interests of the financial institution are adequately protected.

Guidelines

1. Consider the following points prior to entering into any EDP-related service arrangement:
 - Alternative vendors and related costs;
 - Financial stability of the vendor;
 - Requirements for termination of service; and
 - Quality of service provided.
2. Ensure that any contract specifies the duties and responsibilities of the financial institution and the vendor of EDP services.
3. Review the contract's penalty provisions for reasonableness in the areas of: length of

contract, excessive fees, compensation of the servicer for loss of income, etc.

4. Ensure that the following items are included in the service contracts:

- The vendor agrees to submit to an examination by OTS, which will evaluate and monitor the soundness of the vendor in order to limit the institution's risk. The following language should be incorporated in the contract:

"By entering into this agreement the EDP services vendor agrees that the Office of Thrift Supervision will have the authority and responsibility provided to the other regulatory agencies pursuant to the Bank Service Corporation Act, 12 U.S.C. 1867(C) relating to services performed by contract or otherwise."

- The vendor provides the OTS District Director of the district in which the data processing center is located with a copy of the current third party review report when a review has been performed. (See PA-7-1A for guidance concerning third party review report requirements.)
- The vendor provides the OTS District Director of the district in which the data processing center is located with a copy of the vendor's current audited financial statements.
- The vendor agrees to release the information necessary to allow the institution to develop a disaster contingency plan which will work in concert with the vendor's plan.

In addition, institutions should be aware of the FIRREA-imposed restrictions on contracts as outlined in Thrift Bulletin 44, "Interagency Statement on EDP Service Contracts." Also, the provisions of 12 C.F.R. 563.17-1(d) and (e) outline reporting requirements for an institution that elects to maintain any of its records by means of data processing servicers.

The attachment to this Bulletin provides further guidelines for a thrift institution initiating, renewing, or revising a contract or agreement for EDP services.

/s/John F. Downey
Acting Senior Deputy
Director for Supervision

Attachment

Attachment to TB 46

Contracting for Data Processing Services or Systems

While the provisions in an EDP service contract are not standardized across the industry, a number of items are included in most contracts. This attachment contains a list of various provisions which are usually incorporated in EDP servicing contracts. Neither the significant deviation from, or inclusion of, these items will render a contract unacceptable or acceptable. This is an outline and is not meant to be all inclusive.

Provisions contained in an electronic data processing servicing contract may include:

- A detailed description of the specific work to be performed by the servicer, and the frequency and general content of the related reports.
- A fee schedule which outlines development, conversion and processing cost, as well as charges for special requests.
- An outline of the training to be provided for institution personnel, including the type, number of employees to be trained, and the associated cost.
- Established time schedules for receipt and delivery of work.
- The availability of on-line communications, security over accesses and transmissions, and alternate data entry considerations.
- Audit responsibility, including the right of financial institution representatives to perform an audit.
- A definition of backup, contingency, and record protection provisions (equipment, software and data files) to ensure timely processing by the service center in the event of an emergency.
- A detailed description of liability for source documents while in transit to and from the service center. The responsible party should maintain adequate insurance coverage for such liabilities.
- Maintenance of adequate insurance for fidelity and fire liability, reconstruction of physical properties, data reconstruction, and resumption of normal operations, as well as for data losses from errors and omissions.
- Confidentiality of records.
- Ownership of software and related documentation.
- Ownership of master and transaction data files and their return in machine-readable format upon the termination of the contract or agreement.
- Price changes, cost and method of cancellation of the contract, or withdrawal from the servicing arrangement by either party.

-
- Processing priorities for both normal and emergency situations.
 - Mandatory notification by the servicer of all systems changes that affect the institution.
 - A requirement that the vendor be responsible for keeping the software current by incorporating regulatory changes and updates.
 - Access to vendor's source code and maintenance of documentation via escrow agreements for turnkey operations.
 - A guarantee that the servicer will provide necessary levels of transition assistance if the institution decides to convert to other automation alternatives.
 - Cancellation, termination, and bankruptcy clauses.
 - A requirement that the EFT facility provide for contingencies, integrity, security, and confidentiality of data.
 - Financial information (audited) to be provided annually by the servicer to the financial institution.
 - A detailed description of the disaster recovery contingency test results to be provided annually by the servicer to the financial institution.
 - A prohibition against the assignment of the contract by either party without the consent of the other.

Office of Thrift Supervision

Thrift Bulletin 59

Interagency Supervisory Statement on EFT Switches and Network Services

May 19, 1993

Summary:

The Office of Thrift Supervision, Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and the National Credit Union Administration have jointly issued the attached Interagency Supervisory Statement on EFT Switches and Network Services to all federally supervised financial institutions. The statement alerts the board of directors and senior management of financial institutions to the risks associated with switch and network services in electronic funds transfer (EFT) systems. Management of each institution that uses EFT switches and network services should implement policies consistent with this bulletin.

For Further Information Contact:

Your Regional office or the Division of Compliance Programs, Office of Thrift Supervision, Washington, D.C.

/s/John F. Robinson
Acting Deputy Director for Washington Operations

See FFIEC Policies SP-9 for details.

GLOSSARY

CHAPTER 31

(FILE NAME ON DISK # 3 = S4C31.WPD)

A

A.B.A. (American Bankers Association) – A national organization consisting of the voluntary association of banks and other bank organizations.

A.B.A. number – A code number identifying state and federal commercial banks used as an aid in routing unpaid checks in transit. Numerator is assigned A.B.A. number; denominator is transit routing symbol.

Example: A - B

 C D E

- A) 1-49 major city
 50-101 state or territory
- B) Bank number
- C) Federal Reserve district
- D) 2-5 branch of Federal Reserve office
 6-9 special collection code
- E) Payment availability of 1-9 state or federal office

absolute address – See address, absolute.

absolute coding – Coding that uses machine instructions and absolute addresses. It can be executed directly by a computer without prior translation to a different form. Contrast with symbolic coding.

ACH (Automated Clearing House) – A nationwide electronic payment system among financial institutions. ACH entries can be substituted for checks in recurring payments, such as mortgages, or direct deposits, such as federal and corporate benefits payments, including Social Security payments. In an ACH debit entry, the originator *receives* funds; in an ACH credit entry, the originator *pays* funds. Final

settlement is made, generally one or two days after transactions are deposited at the processor through reserve accounts at Federal Reserve banks.

access control list – A list of entities, together with their access rights, that are authorized to have access to a resource.

access method – Technique and/or program code for moving data between main storage and input/output devices.

access mode – A technique used to obtain a specific record from, or to place a specific record into, a file. See also *random access* and *serial access*.

access time – The amount of time required for a computer to locate and transfer a character of data from its storage position and make it available for processing, or to return a character from the processing unit to the storage location.

account – A record of all financial transactions and their dates affecting a particular phase of the business expressed in debits and credits, evaluated in money, and showing the current balance, if any (the excess of debits over credits, or the excess of credits over debits).

accounting controls – Controls concerned with the safeguarding of assets and the reliability of financial records.

account number – The numerical identification number assigned to an account within a given instruction or business. See also *code of accounts*.

accumulator – A device, area or register in a computer for temporary storage of data in an arithmetic or logic operation, and temporary storage of the result.

acoustical coupler – Data communications device that converts electrical data signals to/from tones for

transmission over a telephone line using a conventional telephone handset.

actual address – Same as *address, absolute*.

activity – The degree of frequency with which individual records in a file are used, modified or referred to. For example, an "activity factor" of 0.10 (or 10 percent) denotes that an average of one out of every 10 master file records is referenced or affected by a transaction during a run.

address – The specific location where data is stored in a computer system. A symbolic (numerical or alphabetical) designation of the storage location of the data or machine unit to be used.

address, absolute – A fixed location in the computer's memory which has been assigned to a particular internal storage location. Synonymous with *actual address* or *absolute address*.

address, relative – A memory address that represents some distance from a starting point (base address), such as the first byte of a program or table. The absolute address is derived by adding the relative address to the base address.

address, symbolic – A label to identify a particular location, function or other information in a routine independent of the relative or absolute location of the information in the routine, used for the convenience of the programmer.

advices – The term "advices" connotes several types of forms used in the banking field. Generally speaking, an advice is a form of letter that relates or acknowledges certain activity between a depositor and a financial institution. Examples are credit advice, debit advice, advice of payment, and advice of execution.

algorithmic – Refers to a specific set of defined rules of processes for the solution of a problem in a finite number of steps. Contrast with *heuristic*.

allocate – To assign storage locations to the main routines and subroutines. To fix the absolute machine locations for symbolic addresses.

alphanumeric – A character set that includes both alphabetic characters (letters) and numeric characters (digits). Note: May also contain special characters (dollar signs, commas, etc.).

analog – The use of variable and continuous waveforms to represent information values. See *digital*.

analyst – Person who analyzes and defines business problems and develops computer systems and procedures for their solution.

ancillary – See *auxiliary equipment*.

application – A computer program or set of programs that perform the processing of records for a specific business function, such as demand deposits (DDA), installment loans, mortgages, etc.

application controls – Input, processing and output controls relating to a specific application.

application layer – A logical entity of the open systems interconnection (OSI) model; the top of the seven-layer structure, generally regarded as offering an interface to, and largely defined by, the network user; in IBM's Systems Network Architecture (SNA), the end-user layer.

application program interface (API) – System software that provides resources on which programmers can draw to create user interface features, such as pull-down menus and windows, and to route programs to local area networks (LANS).

application programmer – One who designs, develops, debugs, maintains, and documents computer application programs using various computer languages (COBOL, RPGII, BASIC).

applications server – Runs applications and retrieves information from databases.

application system – A collection of programs and documentation relevant to an application.

ARU (Audio Response Unit) – A device that provides voice response to coded signals.

ASCII (American Standard Code for Information Interchange) – A 7-or 8-bit compatible USA standard code adopted to facilitate the interchange of data among various types of data processing and data communications equipment. See also *EBCDIC*.

assemble – To prepare a machine-language program from a program written in symbolic coding by

substituting absolute operation codes for symbolic operation codes and absolute or relocatable addresses for symbolic addresses. For example, the symbolic instruction ADD TAX might be assembled into the machine instruction 24 1365, where 24 is the operation code for addition and 1365 is the address of the storage location labeled TAX. Same as *compile*.

assembler – A computer program that assembles programs written in symbolic coding into machine-language programs. Note: Assemblers are an important part of the basic software for most computers.

asynchronous communications – A method of data communication in which the transmission of bits of data is not synchronized by a clock signal, but is accomplished by sending the bits one after another, with a start bit and a stop bit to mark the beginning and end of each data unit. Asynchronous communications comes into play when you have only two wires. This form of transmission can be compared to sending eight cars, one after the other, down a one-lane road, with a motorcycle policeman at the beginning and end of the procession. See *synchronous communications*.

audit function – Periodic or continuous verification of the bank's financial records, e.g. assets, liabilities, income, and expenses. This function is performed by the auditor (see definition). The auditor is appointed by the board of directors, and is responsible for carrying out this verification. Among the assets and liabilities more regularly verified are cash, loans, collateral for loans, and savings and checking accounts. Verification may consist of a physical count of the assets as reflected by the general ledger or listing of the balances as shown on each savings or checking account with proof of the total as shown on the general ledger. Direct verification may also be made with borrowers or depositors.

auditor – An officer who is in charge of all audit functions (see definition) and directly responsible to the board of directors.

audit trail – A means of identifying actions taken in processing input data or in preparing an output such that data on a source document can be traced forward to an output (a report, for example) and an output can be traced back to the source items from which it is derived. Note: The audit trail can also be termed an

inquiry trail or a management trail, because it is used as a reference trail for internal operations and management, as well as for audit tests.

authenticate – To establish the validity of a claimed identity, usually with a password.

authentication – The process of proving the claimed identity of an individual user, machine, software component or any other entity. Typical authentication mechanisms include conventional password schemes, one-time passwords, biometrics devices, and cryptographic methods.

AUTOEXEC.BAT – A batch file whose main purpose is to process commands that set up the operating system for DOS. It is automatically carried out whenever the computer is started or restarted. The file contains basic start up commands that help configure the system.

automated system log – A report in which job-related information, operational data, descriptions of unusual occurrences and commands, and messages to or from the operator are listed automatically.

automatic route selection (ARS) – The capability of a switch, typically a private branch exchange (PBX), to automatically determine an optimal route for establishing a circuit; also called least-cost routing (LCR).

auxiliary equipment – Equipment not under direct control of the central processing unit. See *peripheral equipment*.

auxiliary storage – Storage that supplements a computer's primary internal storage. Note: In general, auxiliary storage has a much larger capacity, but a longer access time, than primary storage. Synonymous with *mass storage*. Same as *secondary storage*.

B

backbone network – A term that describes a transmission facility, or an arrangement of such facilities, designed to interconnect lower-speed distribution channels or clusters of dispersed users of devices.

backup – Equipment or procedures that are available for use in the event of failure or overloading of regularly used equipment or procedures. Note: The provision of adequate backup facilities is important to the design of all information processing systems especially real-time systems, where a system failure may bring the total operations of a business to a standstill.

BAI – Bank Administration Institute.

band – (1) A cylindrical area on a magnetic drum; (2) Range of frequency between two defined limits.

bandwidth – The transmission capacity of a computer channel, communications line, or bus. It is expressed in cycles per second (Hertz), the bandwidth being the difference between the lowest and highest frequencies transmitted. The frequency is equal to or greater than the bits per second. Bandwidth is also often stated in bits or bytes per second. In local area networks, bandwidth is a measurement of network speed. In monitors, bandwidth is a measurement of the monitor's maximum resolution; the higher the bandwidth, the more dense the resolution on-screen.

batch – A group of transactions, deposits or check clearings assembled for proving or processing purposes. A batch may consist of from 100-300 checks. See *batch processing*.

batch control ticket – A document accompanying a batch of transaction documents that records such information as batch number, control totals and routing.

batch processing – A method in which items are collected into groups or batches to permit convenient and efficient processing. Note: Records of all transactions affecting a particular master file are accumulated over a period of time (one day, for example), arranged in sequence and processed against the master file.

batch proof – A system for proving deposits, usually performed in the following sequence: (a) deposits are assembled in groups of various sizes; (b) deposit tickets are sorted into one group; (c) checks are sorted into several classifications, such as clearings, transit, bookkeeping; (d) cash release tickets are sorted according to tellers; (e) deposit tickets, checks and cash release tickets are listed on a "batch" or "block"

sheet in their respective columns; (f) deposit and other credit totals should equal the total of all checks and other debits.

batch sheet – A "proof sheet" used in the batch proof system (see definition). The batch sheet is arranged in columns for deposits, various classifications of checks and other debits, and cash release tickets. After sorting, all items in the batch are listed in their respective columns and the totals are recapped and proved. The batch sheet becomes a permanent record of the bank, and is used by auditors to verify any errors arising from transactions.

batch total – A sum of a group of items used to check the accuracy of operations on a particular batch of records.

baud – Measurement of signaling speed indicating line changes per second, where line changes can represent one or more bits. A measure of data transfer speed. Only for line changes representing a single bit, baud is equal to bits per second. Common baud rates in telecommunications are 300, 1200, 2400, 9600, 14,400, or 28,800.

baud rate – A number representing the speed at which information travels over a communication line and/or through a COM serial port.

BCD (Binary Coded Decimal) – A 6-bit data code in which decimal digits are expressed by binary numerals. See *EBCDIC*.

benchmark – A point of reference from which measurement can be made.

binary – A numbering system using only the values 0 and 1. Used by computers for data representation.

biometrics – A method of verifying a person's identity by analyzing a unique physical attribute of a specific person including fingerprints, hand geometry, retinal scanning, voice verification or signature dynamics.

binary – A numbering system that uses only two digits 0 and 1. It is used in computers because it is easier for the machine to understand. Since the memory systems of a computer consist of a series of switches, a binary "0" means that the switch is off and a binary "1" means that the switch is on.

BIOS (Basic Input/Output System) – Provides fundamental services required for the operation of a computer. These routines are generally stored in Read Only Memory (ROM). They control basic hardware operations such as interactions with diskette drive, hard disk drives, and the keyboard.

bit – A binary digit (0 or 1) in the representation of a number in binary notation.

bitmap – A representation of an image by an array of bits. The image is stored as a pattern of dots.

block – A quantity of transmitted information regarded as a discrete unit by size or, more commonly, by its own starting and ending control delimiters. A block usually contains self-contained control, routing, and error-checking information; for example, the data recorded between two interblock gaps on a magnetic tape.

block diagram – See *flowchart*.

blocking – Combining two or more logical records into one block, usually to increase the efficiency of computer input/output operations. For example, the effective data transfer rates of most magnetic tape units can be increased greatly if the need for frequent tape stops and starts is reduced by combining multiple shorter logical records into longer physical blocks.

boundary protection – See *storage protection*.

BPI – Bytes or bits per inch.

branch – 1) An instruction that may cause a departure from the normal sequence of executing instructions, depending on the results of an operation, the contents of a register or the setting of an indicator; 2) A set of instructions executed between two successive conditional transfer instructions.

breakpoint – A specified point in a program at which the program may be interrupted by manual intervention or by a monitor routine. Note: Breakpoints are usually used as aids in testing and debugging programs. They facilitate the halting of a computer or the triggering of a printout at a particular point, so that specific conditions can be examined.

bridge – In local area networks, a device that enables

two networks, even ones dissimilar in topology, wiring, or communications protocols, to exchange data. Bridges are protocol independent; routers are protocol dependent. Bridges are faster than routers because they do not have to read the protocol to glean routing information. See also *router*, *gateway*, and *hub*.

BTAM (Basic Telecommunications Access Method) – Provides the basic functions to control data communication circuits. It supports asynchronous terminals, synchronous communications, and audio response units. BTAM resides in the central computer and is the interface between the front-end-processor and the user-written application. BTAM is an access method that provides support primarily for input operations. It will not perform all tasks that must be executed in most communication networks; therefore, it is not widely used.

budget – An itemized listing of the amount of all estimated revenue that a business anticipates and the amount of all estimated costs and expenses that will be incurred in obtaining the revenue during a given period of time, such as a month or a year.

buffer – A RAM memory storage location that is used to temporarily hold data during communication between two devices. A temporary storage location that provides uninterrupted data flow between devices, such as keyboards and processors, or processors and printers, until the data from one can be accepted by the other. A device that temporarily holds information in memory. This information is lost when the buffer is turned off. Buffers are generally used between a computer and a printer so that the computer will not be tied up the entire time printing is taking place.

bug – A mistake in the design of a program or computer system or an equipment fault.

bulletin board system – Commonly referred to as a BBS (bulletin board system) that users can access through the use of their own computer with modem and a telephone line. The user “calls” the BBS by having his computer dial the telephone number. A computer at the BBS answers the call and connects itself to the calling user. The calling user may perform such actions as view e-mail, chat with other users, download files, and read information.

burst – To mechanically separate continuous form paper.

burst mode transmission – A procedure in which a logical data group is transmitted at one time.

bus – A transmission path or channel; typically an electrical connection, with one or more conductors, wherein all attached devices receive all transmissions at the same time; a local-network topology, such as used in Ethernet and the token bus, where all network nodes "listen" to all transmissions, selecting certain ones based on address identification.

byte – A group of adjacent bits operated on as a unit and usually shorter than a word. Note: In a number of current computer systems, this term stands specifically for a group of eight adjacent bits that can represent one alphanumeric character or two decimal character digits.

C

Carrier-sense multiple access with collision detection (CSMA/CD) – A local-network access-control technique, where all devices attached to a local network listen for transmissions in progress before attempting to transmit; if two or more begin transmitting at the same time, each backs off (defers) for a variable period of time (determined by a set algorithm) before again attempting to transmit.

CASE (Computer-Aided Software Engineering) – A software development technology that is used to automate the software development process and maintenance of software systems. CASE products or tools may be used separately or in an integrated fashion throughout the Software Development Life Cycle (SDLC) process.

CASE repository – The database in which the outputs of the various CASE tools are stored for later use.

cataloging – Placing data sets permanently in a storage device for later use. This technique avoids having to read in a data file each time certain programs or data are needed.

CBCT (Customer Bank Communications Terminal) – Remote electronic devices through which customers

may withdraw, deposit, or transfer funds from or to checking or savings accounts (i.e., automated teller machines and service counter terminals).

CD-R (Compact Disk-Recordable) – A recordable CD-ROM technology using a disk that can be written only once. The disks are 4.72 inches in size and contain thousands of pages of information. For high-capacity storage, CD-R is not expected to replace the larger-disk WORM systems. See *CD-ROM*.

CD-ROM (Compact Disk-Read Only Memory) – These disks are 4.72 inches in size. Their major application is publishing-encyclopedias, directories, catalogs, and other references. A master disk is first produced by a publisher, and multiple copies are reproduced for distribution to users. With appropriate equipment (CD-ROM drives), these disks can be read thousands of times.

CE (Customer Engineer) – A person responsible for field maintenance of computer hardware and software.

central office – The phone company switching facility or center at which subscribers' local loops terminate; handles a specific geographic area, identified by the first three digits of the local telephone number.

central processor – The unit of a computer system that controls the interpretation and execution of instructions. Synonymous with CPU (central processing unit) and mainframe.

channel – An information transfer path within a computer system. In communications, a physical or logical path allowing the transmission of information.

channel bank – Equipment, typically in a telephone central office, that performs multiplexing of low-speed, generally digital, channels into a higher-speed composite channel; the channel bank also detects and transmits signaling information for each channel and transmits framing information so that time slots allocated to each channel can be identified by the receiver.

channel service unit (CSU) – A component of customer premises equipment to terminate a digital circuit, such as Dataphone digital service (DDS) or

T1 at the customer site.

character – One of a set of elementary signals which may include decimal digits 0 through 9, the letters A through Z, punctuation marks and any other symbols acceptable to a computer for reading, writing, or storing.

character density – A measure of the number of characters recorded per unit of length or area.

character recognition – The act of reading, identifying, and encoding a printed character by optical or other automatic means.

character set – A list of characters acceptable for coding to a specific computer or input/output device.

check bit – A binary check digit. Note: A parity check usually involves the appending of a check bit of appropriate value to an array of bits.

check digit – A digit that is calculated from the numbers in an account number, and added to an account number to check the correctness/validity of that number in subsequent use.

check point – A point in a routine at which sufficient information can be stored to permit restarting the computation from that point.

check problems – A problem whose correct results are known. Used to determine whether a computer or a program is operating correctly.

checksum – A method of error detection which is a summation of all the bits in a message and contained in the message. Used for encrypted messages.

CISC (Complex Instruction Set Computer/Computing) – The traditional architecture of a computer that uses microcode to execute very complex instructions. Contrast with *RISC*.

class of service (COS) – Designation for one of several variable network connection services available to the user of a network, usually distinguished by security offered (such as encryption), transmission priority, and bandwidth; the network user designates class of service at connection establishment, typically using a symbolic name mapped into a list of potential routes, any of which

may provide the requested service.

clearings – Checks and other items deposited for exchange with other financial institutions in a clearinghouse arrangement or through the Federal Reserve check clearing system.

client – A single user PC or workstation (front-end) associated with software that provides presentation services as an interface to computing resources. Presentation is provided by visually enhanced processing software, known as a Graphical User Interface (GUI).

client-server computing – A technique with which processing can be distributed between nodes requesting information (clients) and those maintaining data (servers). Similar to a LAN or WAN environment.

client-server network – A method of allocating resources in a local area network, so that computing power is distributed among computer workstations in the network, but some shared resources are centralized in a file server.

CMOS (Complementary Metal-Oxide Semiconductor) – Pronounced “sea moss,” this MOS chip design is used because it costs less, consumes less electricity and can hold more circuitry in the chip than other designs. A CMOS chip is used with battery backup to store the BIOS setting in a personal computer. It tells the computer how to start itself when power is first turned on (Typically 3vDC voltage level). The CMOS runs the computer’s internal clock and calendar for the time and date.

COBOL (Common Business Oriented Language) – A procedure-oriented language developed to facilitate preparation and interchange of programs which perform business data processing functions. Every COBOL source program has four divisions whose names and functions are: (1) Identification Division, which identifies the source program and the output of a compilation; (2) Environment Division, which specifies those aspects of a data processing problem that are dependent upon the physical characteristics of a particular computer; (3) Data Division, which describes the data that the object program is to accept as input, manipulate, create, or produce as output; and, (4) Procedure Division, which specifies the procedures to be performed by the object program by means of English-like statements, such as

"SUBTRACT TAX FROM GROSS-PAY GIVING NET-PAY" or "PERFORM-PROC-A THRU PROC-B UNTIL X IS GREATER THAN Y."

code of accounts – A chart of accounts in which each group (such as Assets) is given a group classification number (such as 1,000) with the second digit of that number (such as 1,000) representing the secondary classification (such as Current Assets) and the remaining digits (such as 01 in the figure 1,101) representing a finer breakdown (such as Cash) of the secondary classification.

code generator – Software that generates programming code from specifications.

coding – (1) An ordered list or lists of the successive instructions which direct a computer to perform a particular process; and (2) the act of preparing a list of coding instructions.

COM (Computer Output Microfilm/Microfiche) – A technology that converts data from a computer into visually readable language and records it on microfilm or microfiche.

communications server – A computer whose primary responsibility is to connect one network to another.

compile – To prepare a machine-language program (or a program expressed in symbolic coding) from a program written in another programming language (usually a procedure-oriented language, such as COBOL or FORTRAN). The compilation process usually involves examining and making use of the overall structure of the program, and/or generating more than one object program instruction for each source program statement. Same as *assemble*.

compiler – A computer program that compiles. Compilers are an important part of the basic software for most computers. However, the computer time required to perform the compilation process may be excessive. In addition, the object programs produced by the compiler may require more execution time and more storage space than programs written in machine language.

computer-aided software engineering (CASE) – See CASE

computer system – A functional unit consisting of one or more computers and associated software.

computer virus – A computer program which embeds itself in other code and can replicate itself. Once active, it takes unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programs.

CONFIG.SYS – This file contains statements that set up the system configuration each time you start or restart the operating system. The commands in this file enable or disable system features, set limits on resources, and extend the operation system functionality by loading device drivers. The operating system adds this file to the root directory during installation.

console – A unit of equipment, usually a video display and keyboard or printer, used by computer operators or maintenance engineers to communicate with the computer.

console operator – The employee charged with the duty of operating or supervising the operation of a control console, including direction of the main computer and all elements of the system directly connected with it.

console run book – A book containing computer operator instructions for a run.

constant-ratio code – A code in which all valid characters have the same number of 1 bits, thereby facilitating the performance of a validity check. For example, in the "4-of-8" code, frequently used in data communications, each of the valid characters is represented by a combination of four 1 bits and four 0 bits.

contention – When a computer terminal has data to send on a multipoint line it selects the terminal's address and then sends it. In a contention environment any location can attempt to transmit data to another location in the network at any time. If the addressed location is not busy, transmission occurs. Other terminals attempting to send data receive a busy signal until the first transmission ends.

context sensitive help – A feature of many programs wherein pressing the hot key (F1) or selecting the menu choice brings up the assistance and information that pertains to the portion of the program that is currently active or the task that is currently being performed.

contingent liability – The term applied to the obligation of a guarantor or accommodation endorser of a negotiable instrument. The guarantor or endorser receives no benefit from the negotiable instrument involved, but is required by law to make good the payment of the instrument if the maker defaults. The actual liability exists with the maker of the note (the borrower). The contingent liability exists for the duration of the instrument, and is passed to the guarantor or endorser as a primary liability only if the borrower dishonors the instrument upon presentation and request for payment.

control account – An account in the general ledger used to carry the total of several subsidiary accounts. Whenever any subsidiary account is affected, the transaction will be reflected in the control account total. Control accounts are also used as "total" accounts, controlling the accounts within a "book" or "ledger" in the bookkeeping department and the savings department.

control clerk – A person performing duties associated with the control over data processing operations. Note: Such duties usually include the checking of control totals, run-to-run totals, and output totals before distribution, etc.

control environment – Management's efforts to exercise direction or restraint over surrounding conditions or influences of the data processing function.

control program – A routine, usually contained within an operating system, that aids in controlling the operation and in managing the resources of a computer system.

core storage – A form of high-speed storage using magnetic cores; part of the CPU; also used to refer to main storage.

correspondent bank – A bank that is the depository for another bank or provides other banking services is known as its correspondent. The correspondent bank accepts deposits in the form of cash letters and collects items for its depositor.

CPU (Central Processing Unit) – Same as central processor.

CPU clock – Used to record the amount of time the

central processing unit takes to execute instructions.

crossfooting test – A programmed check on computer processing in which individual items used in arriving at result items are totaled and the total is compared to an independently derived result total. For example, a total net pay figure reached by subtracting a deduction item total from a gross pay total can be compared with a total net pay figure derived by another method under the program.

cut – An expression used in financial institutions to denote totaling a pack of sorted checks going to one destination. The term is most often used in institutions equipped with proof machines. Since these machines can list a large number of checks on a tape, it is more convenient to "cut a tape" by taking totals at periodic intervals.

cut-off – For better control over a huge volume of checks passing through the proof department in large financial institutions, these institutions have periodic "settlements" or "cut-offs" of work. Each "cut-off" is balanced and items are immediately released from the proof department after each "settlement." This also permits transit items to be mailed in several deliveries each business day.

cycle mailing – The practice of dividing the depositors' accounts into groups termed "mailing cycles," and the mailing of statements at periodic intervals during the month. Proponents of this practice claim that it is more efficient than mailing all depositor statements at one time (usually at the end of the month).

cycle posting – The practice of dividing accounts to be posted into groups termed "cycles" and posting these accounts at periodic intervals during the month.

D

DASD (Direct Access Storage Device) – A peripheral device that is directly addressable, such as a disk or drum. The term is used in the mainframe world. See also *direct access* and *random access*.

database – Data items that are stored in order to meet an organization's information processing and retrieval needs. An organized collection of information that

can be accessed by a computer. Also, describes a category of software programs used to organize and manipulate long lists of data, such as names, addresses, and phone numbers. As you type the list, the software automatically copies it onto a disk (unlike most other software that requires you to activate the "Save" feature to write to disk). You can edit the data list and sort it in any order you wish. Note: The term may refer to an integrated file used by many processing applications, as opposed to an individual data file for a particular application.

database server – A computer that stores data centrally for network users and managers, and often uses client-server software to distribute the processing of that data between itself and nodes requesting information.

data capture – The process of recording data on machine-readable tape and/or disk type media as a by-product of transaction processing. In point-of-sale systems, it refers to functions performed by a terminal or computer in capturing information relative to a sale. The information captured is stored in a data base. It can then be accessed for providing audit trails, printing statements for customers, and other purposes.

data circuit-terminating equipment (DCE) – In a communications link, equipment that is part of the network, an access point to the network, a network node, or equipment which a network circuit terminates; in the case of an RS-232-C connection, the modem is usually regarded as DCE, while the user device is data terminal equipment (DTE); in a CCITT X.25 connection, the network access and packet switching node is viewed as the DUE.

data collection – Act of bringing data from one or more points to a certain point.

data compression – A software technique used to increase the amount of data stored on a hard disk. Data compression utilities reduce the space needed to store individual files, thereby increasing the number of files that can be stored in a given space. A compressed file cannot be used until it is expanded to its original form.

data concentrator – A piece of hardware that collects data at an intermediate point from several low and medium speed lines for retransmission across high-

speed lines.

data conversion – Process of changing data from one form of representation to another, such as converting written source documents to machine-readable form by keypunching or data entry.

data dictionary – The database that describes data and its attributes.

data element – A piece of information carried in a program or data file. May be a bit character field or a data string.

Data Encryption Standard (DES) – U.S. government standard for data encryption method published by the National Institute of Standards and Technology for the encryption of sensitive U.S. Government data that does not fall under the category of national security related information. The DES uses a 64-bit key consisting of 56 independent bits and 8 others which may be used for parity checking.

data file – A collection of related data records organized in a specific manner for a particular application.

data link layer – Establishes, maintains, and releases data links and ensures error-free transmission; invokes retransmission when errors are detected.

data phone – An AT&T designation for a service that provides data communications over telephone facilities.

data reduction – The use of arithmetic, mathematical or statistical techniques to obtain or extract only needed information from a larger mass of related information.

data scope – See *oscilloscope*.

data set – A collection of related data. See *file*.

data terminal equipment (DTE) – Generally end-user devices, such as terminals and computers that either generate or receive the data carried by the network; in RS-232 connections, designation as either DTE or DCE determines signaling role in handshaking; in a CCITT X.25 interface, the device or equipment that manages the interface at the user's premises.

data transmission – The sending of data from one part of a system to another part.

DBMS (Data Base Management System) – A comprehensive software system that builds, maintains, and provides access to common data items that can be processed by one or more application programs. This software establishes and employs rules about system file organization and processing and establishes relationships between files and "records" in each file. This provides for integration or sharing of common data items that can be processed by one or more application programs; can be hierarchical, network or relational in structure.

DDBMS (Distributed Data Base Management System) – A data base which is spread across several, possibly remote, computers which are interconnected by a communications network.

debug – To trace and eliminate mistakes in a program or faults in equipment. Synonymous with *troubleshoot*.

decision table – A table listing all the contingencies to be considered in the description of a problem, together with the corresponding actions to be taken. Note: A decision table permits complex decision-making criteria to be expressed in a concise and logical format. It is sometimes used in place of flowcharts for problem definition and documentation. Compilers have been written to convert decision tables into programs that can be executed by computers.

decollate – A term used in the computer industry when referring to the separation of carbon paper from the hardcopy original computer paper and the hardcopy duplicates. Computer paper for trial balance reports and other supporting reports normally consists of one original and multiple copies with carbon paper between each page. Most centers have decollating machines to remove the carbon paper, while others complete this process by hand.

desk checking – A manual checking process in which representative data items are traced through the program to detect errors in program logic.

destructive update – A file posting procedure in which the output file is created on the same physical media that contained the input file, thus destroying the input file. See *update*.

detail file – A file containing relatively transient

information. For example, records of individual transactions that occurred during a particular period of time. Synonymous with *transaction file*. Contrast with *master file*.

diagnostics – Messages that are output from the compiler or assembler, indicating possible errors in the source program.

diagnostic routine – A routine designed to perform diagnostic functions. See also *dump*, *post-mortem routine*, *snapshot* and *trace routine* (commonly used types of diagnostic routines).

dial-back – A security method in which a user dials-up a system for access; the system verifies the user call and calls back at a predetermined phone number.

dial-up – The ability of a remote user to access a system by using private or common carrier telephone lines.

difference account – An account carried in the general ledger where all differences from the true balance of the daily business of the financial institution are recorded. Overages and shortages of all departments are recorded in this account. In large institutions, a difference account may exist for each department, and the net total of these subsidiary difference accounts will balance to the general ledger control.

digit – A single symbol or character representing a quantity.

digital – Referring to communications processors, techniques, and equipment where information is encoded as either a binary "1" or "0"; the representation of information in discrete binary form, discontinuous in time, as opposed to the analog representation of information in variable, but continuous, waveforms.

digital signatures – Data appended to or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery by the recipient.

direct access – Pertaining to a storage device where data or blocks of data can be read in any particular order. See *random access*.

direct verification – A method of financial institution audit whereby the auditor sends a request for the verification of the balances of accounts as of a stated date to the customers. Verifications are returned and directed to the auditor confirming the correctness of balances or listing discrepancies.

disk – A physical element for direct access storage.

disk pack – A removable direct access storage media containing several magnetic disks on which data is stored.

disk storage – A storage device which uses magnetic recording on flat rotating disks.

Distributed Transaction Processing (DTP) – Distributed application processing involves multiple users requiring access to a single shared resource concurrently. An example is a bank application containing customer accounts which require multiple access for both reading and update operations.

dormant accounts – Accounts that have had no customer originated activity for a stipulated period. See also *inactive accounts*.

DOS (Disk Operating System) – Software that directs the flow of data between disk drives and a computer. It acts like a “Traffic Cop” to control the flow of information to and from application software.

downtime – The elapsed time when a computer is not operating correctly because of machine failure.

drum storage – A direct access storage device which uses magnetic recording on a rotating cylinder. A type of addressable storage associated with some computers.

dual read – The use of two separate reading stations to read the same record. Results of the two operations are compared to detect reading errors.

dumb terminal – See *terminal*.

dump – (1) To copy the contents of a set of storage locations, usually from an internal storage device (such as core storage) to an external storage medium (such as magnetic tape) and usually for diagnostic or rerun purposes; (2) data that results from the process defined in (1). See also *post-mortem routine*, *selective*

dump and *snapshot*. Synonymous with *storage dump*.

duplex channel – A channel providing simultaneous transmission in both directions.

E

EBCDIC (Extended Binary Coded Decimal Interchange Code) – An 8-bit code that represents an extension of the 6-bit “BCD” code widely used in computers of the first and second generations. Note: EBCDIC can represent up to 256 distinct characters and is the principal code used in many current computers. See also *ASCII*.

echo check – A check upon the accuracy of a data transfer operation in which data received (usually by an output device) is transmitted back to its source (usually a control unit) and compared with the original data. For example, an echo check on an output operation usually can verify that the proper print hammers or punch pins were actuated at the proper moments. However, it cannot ensure that the proper marks were actually recorded on the output medium.

edit – To modify the form or format of data. This may involve the rearrangement, addition (for example, insertion of dollar signs and decimal points), and deletion (for example, suppression of leading zeros) of data, code translation and control of layouts for printing (for example, provision of headings and page numbers).

edit routines – Routines used to verify the accuracy or reasonableness of data. Also used to modify the form or format of data. This may involve the rearranging, adding (inserting dollar signs and decimal points) and deleting (suppressing leading zeros) data.

Electronic Bulletin Boards (EBBs) – A computer with special software so that it can be accessed by anyone with a modem and phone line. Callers may put notes and messages on the EBB through their computer or may read any messages or notes left by other users. These can be run as a commercial enterprise (for fee) or by hobbyists (usually at no cost). See *bulletin board system*.

EDP (Electronic Data Processing) – An all inclusive term liberally interpreted to mean the overall process of converting data by electronic means to any desired form.

EFTS (Electronic Funds Transfer System) – Various computerized electronic communications systems which transfer financial information from one point to another.

Electronic Mail (E-Mail) – Software on several computers on a network which facilitates the passing of messages from one user of the network to another.

emulator – A device usually used in conjunction with special routines that enables a computer to execute, without prior translation, machine-language programs written for another computer of dissimilar design. Note: Emulation is a method for achieving program compatibility between computers produced by the same or different manufacturers.

encryption – The process of scrambling data by a device or encoding principle (mathematical algorithms) so that the data cannot be read without the proper codes for unscrambling the data.

end-to-end-accountability – The property that ensures that the actions of an entity from initial system logon to system logoff may be traced uniquely to the entity even when those actions take place across a distributed system or network.

entry – The original record made in account books, also the items so entered. In double entry bookkeeping, an entry is incomplete if the total value of the debits and credits used to complete the records of a given transaction are not equal.

error correcting code – An error detecting code that uses additional code elements (e.g., additional bits), so that if a certain type of error occurs, the mutilated representation can be analyzed and corrected. Note: An erroneous correction may result if an error occurs that the code has not been designed to correct.

error detecting code – A code in which each representative or character conforms to specific rules of construction, so that if certain types of errors occur, the mutilated representation will not conform to the rules of construction. Thus, the presence of errors can be detected without reference to the

original message. Note: Each of the most common types of error detecting codes appends a parity bit to each array of bits and uses a parity check. Synonymous with *self-checking code*.

exception reports – Reports which list or flag only those items that exceed a specified range of acceptable values. Also, reports of extraordinary or particular circumstances and activity.

execute phase – An alternate part of the computer's operation cycle where a command in the program register is performed upon the address indicated. The act of performing a command.

executive routine – A routine designed to organize and regulate the flow of work in a computer system by initiating and controlling the execution of other programs; a principal component of most operating systems. Synonymous with *supervisory routine* and *supervisor*.

expanded memory – RAM memory above 1 megabyte that can be used by DOS and some DOS programs in addition to conventional memory.

extended memory – RAM memory that begins above 1 megabyte.

external label – An identifying label attached to the outside of a file media holder; for example, a paper sticker attached to the side of a reel containing a magnetic tape file.

external storage – A storage device outside the computer which can store information in a form acceptable to the computer, e.g., cards, tapes.

F

facilities management – An arrangement whereby a third party operates a bank's data processing department, usually under a multi-year contract.

fetch protection – Prevents one program from accessing the core storage of another program when locating the next instruction in memory for execution by the CPU. See *storage protection*.

fiber optic cable – Glass or plastic fibers over which modulated light pulses from laser or LED (Light Emitting Diode) can transmit data. It is not subject to interference or electronic eavesdropping.

fidelity bond – A bond covering the risk of loss because of larceny, embezzlement, or culpable negligence.

field – (1) a subdivision of a computer word or instruction (for example, a group of bit positions within an instruction that hold an address); or (2) a subdivision of a record, that is, an item.

file – A collection of related records, usually (but not necessarily) arranged in sequence according to a key contained in each record. (Note: A record, in turn, is a collection of related items; an item is an arbitrary quantity of data that is treated as a unit. In payroll processing, an employee's pay rate forms an item, a set of all items relating to a particular employee forms a record, and the complete set of employee records forms a file.)

File Allocation Table (FAT) – A table used by DOS to allocate disk space for a file. It also locates and chains together parts of the file that may be scattered on different sectors, so that the files can be used in a random or sequential manner.

file label – A label identifying a file. Note: An internal label is recorded as the first or last record of a file and is machine-readable. An external label is attached to the outside of the file holder and is not machine-readable.

file maintenance – The updating of files to reflect the effects of nonperiodic changes by adding, altering or deleting data; for example, the addition of new programs to a program library on magnetic tape.

file processing – The periodic updating of master files to reflect the effects of current data, often transaction data contained in detail files; for example, a weekly payroll run updating the payroll master file.

file protection ring – On older computer systems, the absence or presence of a removable plastic or metal ring which (depending on the computer manufacturer) prevents writing on a magnetic tape and thereby prevents the accidental destruction of a magnetic tape file.

file server – A high capacity disk storage device or a computer that stores data centrally for network users and manages access to that data. File servers can be dedicated so that no processes other than network management can be executed while the network is available. File servers can be nondedicated so that standard user applications can run while the network is available.

fine sort – A term used to describe the act of sorting transaction media into numerical or alphabetical order.

firewall – A network node set up as a boundary to prevent traffic from one segment to cross over into another. Commonly used to separate the Internet portion of a company's network from the remainder of the network. See *router* and *bridge*.

fixed-length record – A record that always contains the same number of characters. Note: Restriction to a fixed length may be deliberate in order to simplify and speed processing, or it may be dictated by the characteristics of the equipment used. Contrast with *variable-length record*.

flag – Any of various types of indicators used to denote the existence of a condition.

flashcard – A device for the storage of information usually associated with lap-top or notebook computers.

flow – A general term to indicate a sequence of events.

flowchart – A programming tool to graphically present a procedure by using symbols to designate the logic of how a problem is solved. An example would be a block diagram.

format – An arrangement of information on a form or in storage.

FORTRAN (Formula Translating system) – A procedure-oriented language designed to facilitate the preparation of computer programs that perform mathematical computations. Note: Designed by IBM in the 1950s to use symbols and expressions similar to those of algebra, FORTRAN was not originally intended to be a common language. However, it has evolved through several basic versions (FORTRAN

I, FORTRAN II, FORTRAN IV, etc.) and numerous dialects. It has become largely machine-independent and has recently been approved as a USA standard programming language in two versions (FORTRAN and Basic FORTRAN). FORTRAN is now being employed effectively in certain business as well as scientific applications.

4GL (Fourth Generation Language) – Commercial software which allows a nonprogrammer to formulate English-like commands and queries without having to form a complex programming code.

frame – A group of bits sent serially over a communications channel; generally a logical transmission unit sent between data-link-layer entities that contains its own control information for addressing and error checking; the basic data transmission unit employed with bit-oriented protocols, similar to *blocks*.

frame relay – A high-speed packet switching protocol used for wide area networks (WANs). It is faster than traditional X.25 networks, because it was designed for today's reliable circuits and performs less rigorous error detection. It provides for a granular (customizable) service up to DS1 rates of 1.544 Mbps and is suited for data and image transfer. Because of its variable-length packet architecture, it is not the most efficient technology for real-time voice and video.

front end processor – Typically, a minicomputer used in input processing prior to batch processing or to control data communications networks and terminals in on-line systems.

G

garbage – Unwanted and meaningless information.

gateway – A computer that performs protocol conversion between different types of networks or applications. For example, a gateway can connect a personal computer LAN to a mainframe network. An electronic mail, or messaging, gateway converts messages between two different messaging protocols. See *bridge*.

general controls – Controls common to several

applications, such as operation controls and access controls. Contrast to *application controls*.

generate – To produce, develop, and prepare a program from a set of specifications.

generator – A computer program designed to construct other specialized programs; for example, a report program generator or a generator of data transcription routines. Note: Basing its decisions upon parameters supplied to it, a generator usually selects from among various alternatives the method most suitable for performing a specified task. It then adjusts the details of the selected method to produce a program matched to the characteristics of the data to be handled.

grandfather, father, son cycle – The creation and storage of three generations (or versions) of master files, so that records can be reconstructed in the event of loss of information stored on a magnetic tape.

group – A named collection of logon IDs.

GUI (Graphical User Interface) – A graphical-based user interface that incorporates icons, pull down menus, and a mouse. Designed to make use of a computer easier, because user interactions are consistent, applications communicate effectively, and the GUI hides the complexity of the system.

H

hard copy – Machine output in a visually readable form (usually paper).

hardware – Refers to physical equipment (as opposed to the computer program), for example, mechanical, magnetic or electronic devices. Contrast with *software*.

hash total – A numerical summation of one or more corresponding fields of a file that would ordinarily not be summed.

head – A device that reads, records, or erases data on a storage medium, e.g., a small electromagnet used to read, write, or erase data on a magnetic drum or tape, or the set of perforating, reading, or marking devices used for punching, reading, or printing on paper tape.

header – Control information and codes that are appended to the front of a block of user data for control, synchronization, routing, and sequencing of a transmitted data frame or packet.

header label – A machine-readable record at the beginning of a file containing data identifying the file and data used in file control.

heuristic – Pertaining to exploratory methods of problem solving in which solutions are arrived at by an interactive, self-learning method. Contrast with *algorithmic*.

hexadecimal – A number system with a base, or radix, of 16. The symbols used in this system are the decimal digits 0 through 9 and six additional characters represented with the letters A, B, C, D, E, and F. Computer programmers use this number system extensively.

high-level data link control (HDLC) – CCITT-specified, bit-oriented, data-link-control protocol; any related control or data links by specified series of bits, rather than by control characters; the foundation on which most other bit-oriented protocols are based.

high-level language – A computer programming language in which each statement represents several binary code instructions. The statements are familiar and common terms used with computers.

housekeeping – Operations in a program or computer system that do not contribute directly to the solution of user's problems, but are necessary to maintain processing control.

hold – A term given to the act of restricting withdrawal of funds from an account.

holdovers – A term used, usually in large financial institutions, to describe a portion of work that has to be processed by a second shift or a night force. Since the business day starts officially at midnight, work which has not been processed by the second shift is "held over" for the night shift to process the remaining work. The work, for control purposes, is credited to the second shift, and recharged as "holdovers" to the night shift.

hub – A central connecting device in a network that joins communications lines together in a star

configuration. Passive hubs are connecting units that add nothing to the data passing through them. Active hubs, also sometimes called multiport repeaters, regenerate the data bits to maintain a strong signal, and intelligent hubs provide added functions. Hubs can provide bridging between LAN types; for example, Ethernet, Token Ring and FDDI.

hypertext – Linking related information. For example, by selecting a word in a sentence, information about that word is retrieved if it exists, or the next occurrence of the word is found.

I

identification – A unique name or number assigned to an individual user accessing a system or a resource.

IDP (Integrated Data Processing) – Data processing by a system that coordinates a number of previously unconnected processes to improve overall efficiency by reducing or eliminating redundant data entry or processing operations; for example, a system in which data describing orders, production, and purchases are entered into a single processing scheme that combines the functions of scheduling, invoicing, and inventory control.

image – An exact logical duplicate stored in a different medium.

imaging systems – The technology used to capture, index, store, and retrieve electronic images of paper documents. The main method of capturing images is by scanning the documents, and turning them into a matrix of dots.

inactive account – An account that has no customer-generated activity. The balance may be stationary, neither deposits nor withdrawals having been posted to the account for a period of time. See also *dormant accounts*.

Index – gives the requestor the location of an image.

infirmity – Any known act, or visible omission in detail, in the creation or transfer of title that would invalidate an instrument. Common examples of infirmities that would cause a financial institution to

refuse payment, if detected, are endorsement missing, signature missing, amount conflicting in written and numerical figures, alteration, or forgery.

information security officer – The person responsible for ensuring that security is provided for and implemented in a computer system from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal.

information system (IS) – A system that consists of people, machines, and methods organized to accomplish specified operations on data that represent information.

information technology – A general term applied to the gathering, storing, processing, and communication of information.

input – Data to be processed. Also the transfer of data to be processed from keyboard or an external storage device to an internal storage device.

input area – The area of internal storage into which data is transferred from external storage.

Integrated Services Digital Network (ISDN) – Protocols used for carrying voice, data, facsimile, and video signal across a single network.

intelligent terminal – A terminal that can be programmed independently by the user.

interactive – An application in which each entry elicits a response, as in an inquiry system or an airline reservation system. An interactive system may also be conversational, implying continuous dialogue between the user and the system.

interblock or interrecord gap – The distance on a data medium, such as magnetic tape, between the end of one block or record and the beginning of the next. Note: Within this distance, the tape can be stopped and brought up to normal speed again. Since the tape speed may be changing, no reading or writing is permitted in the gap.

interface – A common boundary between automatic data processing systems or parts of a system defined by common physical interconnection characteristics, signal characteristics and meanings of interchanged

signals.

interleave – To insert segments of one program into another program, so that the two can be executed simultaneously.

interlock – A protective facility that prevents one device or operation from interfering with another; for example, the locking of a console typewriter's keys to prevent manual entry of data while the computer is transferring data to the typewriter.

internal label – Normally, the first record on a data file, used as a check to ensure that the proper records are being processed.

Internet – A system of connected networks including those of the National Science Foundation and the Advanced Projects Research Agency.

interrupt – A signal, condition, or event that causes an interruption; for example, the completion of an input or output operation, the detection of incorrect parity, or the attempt to execute an illegal instruction or to write in a protected location.

interruption – A temporary suspension in executing a sequence of instructions resulting from the occurrence of a prescribed event or condition (e.g., an *interrupt*). Note: An interrupt usually triggers an unconditional transfer to a predetermined location, where a special routine (usually part of an operating system) determines the cause of the interruption, takes appropriate action and returns control to the point where the program was interrupted (or, in some cases, to another program of higher priority). Effective interruption facilities are vital in computers that operate in multiprogramming or real-time mode.

I/O – Abbreviation for input/output.

IOCS (Input/Output Control System) – A standard routine or set of routines (part of the supervisor) designed to initiate and control the input and output processes of a computer system, thereby making it unnecessary for users to prepare detailed coding for these processes. A supervisor may contain both logical and physical IOCS routines.

ISDN (Integrated Services Digital Network) – A method of high speed digital telecommunication that can be used to transmit and receive voice, data, and

images over existing telephone lines.

IRG (Interrecord Gap) – Same as *interblock gap*.

isochronous transmission – Combines the elements of both synchronous and asynchronous data transmission.

item – Any media, excluding coin and currency, handled daily by a financial institution, the amount or amounts of which, as expressed thereon, will be posted in total, or in detail, as a debit or credit to an institution's account. Items are generally referred to by their type, as "cash items," "transit items," "on us items," "clearing items," "general ledger items," etc.

J

JCL (Job Control Language) – A programming language used to code job control statements. These statements supply information to the operating system and to operators about the program, e.g., name of user, how much memory is required, estimated run time, priority.

job accounting – A function that accumulates accounting software information for each job step to be used for changing use of the system, planning new applications, and supervising system operations more efficiently.

job queuing – A procedure in which programs are read into the computer and await execution until sufficient core storage and peripheral equipment are available.

K

K (kilobyte) – Term used to measure computer storage capacity; one K equals 1,024 bytes or characters.

key – One or more characters associated with a particular item or record and used to identify that item or record, especially in sorting or collating operations. Note: A key may or may not be attached to the record or item it identifies. Contrast *label* and *tag*.

kite – A scheme in which a depositor with accounts in two or more financial institutions takes advantage of the time required for checks to clear to obtain unauthorized credit.

L

label – One or more characters used to identify a program statement or a data item.

LAN (Local Area Network) A system of software and hardware (computers, printer, etc.) and a communications network that links personal and other computers. It is connected by a common data transmission medium (cable) and limited to a geographical area less than about 10 kilometers. Two or more computers connected for local resource sharing. It is made up of servers, workstations, a network operating system, and a communications link. Contrast with *WAN (Wide Area Network)*.

language – A defined set of characters which are used to form symbols, words, etc., and the rules for combining these into meaningful communication, e.g., Algol, FORTRAN, COBOL, Assembler.

Large Scale Integration (LSI) – A technology of chip manufacturing for CPU's and other large microprocessors.

lateral parity check – Same as *row parity check*.

layout – The overall plan or design, such as flowcharts or diagrams, format for card columns or fields, or a procedure outline.

library – A collection of available computer programs and routines.

library routine – A proven routine maintained in a program library (as opposed to a routine written especially for a particular job).

limit test – A programmed check for errors in input data or processing. Note: For this test, a data item is compared with a test amount larger (or smaller) than the data item should be if it is correct. If the checked item is larger (or smaller) than the test amount, an error is indicated.

line printer – A printer in which an entire line of

characters is composed and determined within the device prior to printing.

link – An interconnection.

linkage – The interconnections between two separately coded routines, i.e., entry and exit for a closed routine from the main routine.

linkage editor – A utility program that takes as its input object modules and produces a machine language load (fully executable) module. It formally unites references between program modules and libraries of subroutines.

list – A column of figures listed on an adding machine tape or piece of paper. The term is common in financial institutions, especially in proof, transit and bookkeeping departments where lists are constantly used. Lists are used in obtaining totals for a large volume of items in the same category, such as checks drawn on the same account. The total is posted or used in clearing exchanges or transit letters.

log – A record of the operations of data processing equipment, listing each job or run, the time required, operator actions, and other pertinent data.

logic diagram – Same as *program flowchart*.

longitudinal parity check – A parity check performed on the bits in each track of magnetic tape or punched tape. Note: For this check, the parity bits generated for each of the tracks are recorded simultaneously at the end of each block, in the form of a "longitudinal check character." This is regenerated and checked when the block is read. Synonymous with *track parity check*.

loop – A sequence of instructions that can be executed repetitively, usually with modified addresses or modified data values. Note: Each repetition is called a cycle. Cycling continues until a specified criterion is satisfied (for example, until a counter reaches a predetermined value). The use of loops greatly facilitates the coding of any reiterative process.

LOWER CASE – Term used to describe CASE software modules which automates later stages of software development (programming, testing, and

implementation). These are also referred to as back-end tools and have been more widely used and accepted as traditional programmer productivity aids. Case tools in this category would be code generator and test generator software.

M

machine language – A computer's native language of binary code using 0's and 1's. All executable programs are converted into the binary code of machine language so the computer can process the information.

macro instruction – An instruction that has no equivalent operation in the computer and is replaced in the object program by a predetermined set of machine instructions. Note: Macro instruction facilities can ease the task of coding by precluding the need for detailed coding of input and output operations, blocking, format control, error checks, etc.

macro programming – The process of writing machine procedure statements in terms of macro instructions.

magnetic disk – A flat circular plate with a magnetic surface on which data can be stored in the form of magnetized spots.

magnetic media – Devices used to store computer records; i.e., tape or disk.

marking – The physical notation of a sensitivity label, usually on a document.

mechanism – An operating system entry point or separate operating system support program that performs a specific action or related group of actions.

mainframe – A large computer. Originally, the term referred to the CPU cabinet. Now it refers to a large computer system.

maintenance programmer – Person responsible for periodic updates in various programs.

manual input – The manual entry of data into a device to convert it to electronic form at the time of processing.

mass storage – Large capacity storage that supplements a computer's primary internal storage.

master file – A main reference file of information used in a computer system. It provides information to be used by the program and can be updated and maintained to reflect the results of the processing operation.

matrix – Items arranged in an array or pattern.

media – Media can be classified as source, input and output. Checks are an example of source media. Input media can be punched tape or cards and magnetic tape. Output media can be punched tape, cards or magnetic tape.

megacycle – One million cycles per second.

memo posting – A systems technique in which transactions are posted to a temporary file before permanent master files are updated. For example, large deposits or withdraws may be posted to a temporary balance file throughout the day, but the master file is updated at the close of the day only from the transaction documents.

memory layout – A diagram showing the assignment of internal storage locations for various purposes (storage of input or output record, storage of constants, etc.).

merge – To form a single sequence by combining two or more similarly sequenced files. Note: Merging may be performed by a computer system for which a merge routine is available. The repeated merging, splitting, and reemerging of records strings can be used to arrange them in sequence. This process, known as a merging sort, is often used as the basis for sorting operations on computer systems.

MICR (Magnetic Ink Character Recognition) – Check routing account number and dollar information is encoded in MICR at the bottom of checks.

microfiche – Computer-generated media, similar to microfilm, used to record data.

microfilm – A roll of film used in a machine to photograph various records.

microsecond – One millionth of a second; one

thousand nanoseconds.

middleware – A client/server specific term used to describe a unique class of software by client/server applications. This software resides between an application and the work and manages the interaction between the GUI front-end and data servers in the backend. It facilitates the client/server connections over the network and allows client applications to access and update remote databases and mainframe files.

milestone – A reference point used to establish when steps in a process are complete.

millimicrosecond – See nanosecond.

minicomputer – A low cost, programmable computer with limited storage capacity.

mis-sent item – An item that has been sent in error to another financial institution.

mis-sort – An item or check that is sorted into the wrong account. A mis-sent item leaves the financial institution, while a mis-sorted item remains in the financial institution's possession, but causes a control problem.

mnemonic code – A technique to assist the human memory. A mnemonic code resembles the original word and is usually easy to remember, i.e., MPY for multiply and ACC for accumulator.

modem (modulator-demodulator) – A device that converts digital and analog signals into soundwaves that can be sent via telephone lines. The process is reversed for soundwaves from phone lines into impulses for the terminal. This device that permits computers to communicate with one another over telephone lines.

module – A program unit that is discrete and identifiable for compiling, combining with other units, and loading.

monitor – To control the operation of several unrelated routines and machine runs so that the computer and computer time are used advantageously.

monitor routine – 1) A routine designed to indicate

the progress of work in a computer system; and 2) formerly, same as executive routine.

multidrop – In a multidrop network, one terminal is the master or primary station and the rest are secondary stations. A failure on a secondary station will not prevent the data from being transmitted to the other stations. Each station has its own address. No two stations can transmit at the same time.

multilink – In a multilink network the data travels from point A to point B and then to point C, to point D etc. If one terminal on the link fails, all subsequent terminals are affected.

multimedia – The combining of different elements of media (text, graphics, sound, video) for display and control from a personal computer.

multiplexer – A physical device that allows simultaneous transmission of more than one message per line in a teleprocessing system.

multiplexer channel – Low-speed channel capable of two-way transmission.

multipoint – In a mult point network the data flows from point A to point B, from point A to point C, point A to point D, etc. It also flows from points B, C, and D to A.

multiprocessing – Two or more computers linked together, with simultaneous processing of programs each resident in one of the computers. Each computer may run independently or all may access the storage area of another linked computer.

multiprocessor – A computer with more than one Central Processing Unit (CPU) that can be accessed simultaneously by an operating system adapted to this architecture.

multiprogramming – Since the CPU is usually the fastest component in the computer system, multiprogramming attempts to balance the CPU's speed with slower peripherals by allowing several computer programs to run on the computer system at the same time.

MVS (Multiple Virtual Storage) – Introduced in 1974, the primary operating system used on IBM mainframes (the others are VM and DOS/VSE). MVS

is a batch processing oriented operating system that manages large amounts of memory and disk space. Online operations are provided with CICS, TSO, and other system software. MVS/XA (MVS/eXtended Architecture) manages the enhancements, including 2GB of virtual memory, introduced in 1981 with IBM's 370/XA architecture. MVS/ESA (MVS/Enterprise Systems Architecture) manages the enhancements made to large scale mainframes, including 16TB of virtual memory, introduced in 1988 with IBM's ESA/370 architecture. MVS/ESA runs on all models of the System/390 ES/9000 product line introduced in 1990.

N

nanosecond – One billionth of a second.

negative verification – The method of direct verification where the absence of reply indicates a correct balance. See *direct verification*.

network – A group of computers connected by cables or other means and using software that enables them to share equipment and exchange information. A system of software and hardware connected in a manner to support data transmission. An arrangement for interconnecting a number of computers and allowing them to share information and peripheral devices.

network administrator – The person responsible for the installation, management, and control of a network.

network architecture – A description of data formats and procedures used for communication between nodes.

network layer – Exchange of information between two entities over network connections. This layer insulates routing and switching considerations from the rest of the network. Routing between nodes with no direct connection is controlled by querying intermediate nodes to determine a route between the non-physically connected nodes.

network topology – The arrangement of nodes usually forming a star, ring, tree, or bus pattern.

node – Any device, including servers and workstations, connected to a network. Also, the point where devices are connected.

noise – Any extraneous and unwanted signal disturbances in a communications link (e.g., electromagnetic interference, or EMI); usually, random variations in signal voltage or current, or interfering signals.

nonbank servicer – A third party data processing servicer that is not a department or subsidiary of a bank.

O

object – Anything in a computer environment that a subject can act upon, such as in computer security, anything to which access is controlled; for example, a file, program, area of main storage.

object language – A machine language that is the output from a translation process using a compiler or assembler program. Contrast with *source language*.

object program – A program expressed in an object language; for example, a machine-language program that can be directly executed by a computer.

object reuse – The ability to access residual information that is left behind on recycled storage media when a job or activity terminates.

OCR (Optical Character Recognition) – A technology used to convert text in a graphical image into a word processor format that can be used by a computer. OCR is frequently combined with scanners to scan documents into a computer and convert the resulting information into textual data.

off-line – Pertaining to equipment or devices that are not in direct communication with the central processor of a computer system. Note: Off-line devices cannot be controlled by a computer except through human intervention. Contrast with *on-line*.

on-line – Pertaining to equipment or devices that are in direct communication with the CPU. On-line equipment includes readers, line printers, and terminals. In on-line processing, a user has direct and

immediate access to a computer system via terminal devices.

OOP (Object Oriented Programming) – A programming concept that uses objects as the basic components of a program. Objects are modules that contain both data and the instructions/procedures that operate on the data. Examples of OOP are C++ and ADA.

operating system (O/S) – Software required to manage the hardware and logical resources of the system. Software that controls the execution of computer programs. An organized collection of routines and procedures for operating a computer. Functions performed include: (1) scheduling, loading, initiating, and supervising the execution of programs; (2) allocating storage; (3) initiating and controlling input/output operations; and (4) handling errors, etc.

operations manual – The manual that contains instructions and specifications for a given application. Typically includes components for operators as well as programmers. A log section may also be included.

optical scanning – A technique for machine recognition of characters by their images.

oscilloscope – Test instrument that displays electronic signals (waves and pulses) on a screen. It is used to test, analyze, and monitor communication lines.

OSI Model – Model for network communications developed by the International Standards Organization (OSI); identifies functional layers that are isolated by strict interface specifications.

output – A process of transferring data from internal memory to external storage or display. Reports and documents, or tape and disk files are typical examples of output media.

output area – The area of internal storage from which data is transferred to external storage.

overhead – Nonproductive processing that occurs when the operating system and programs are performing administrative tasks, but no production work.

overlay – A technique for bringing routines into memory from magnetic storage during processing, so that several routines will occupy the same storage locations at different times. Overlay techniques are used when the total storage requirements for instructions exceed available memory storage.

owner – The user who controls the access rights to a resource.

P

pack – To combine two or more units of information into a single physical unit to conserve storage.

packet switching – A data transmission method that routes packets along the most efficient path and allows a communication channel to be shared by multiple connections. User information is segmented and routed in discrete data envelopes called packets, each with its own appended control information for routing, sequencing, and error checking. It allows for more efficient use of communication channels.

page – In virtual storage systems, a fixed-length block of instruction, data or both, that can be transferred between real storage and external page storage; typically about 4 K bytes. A program is divided into pages to minimize the total amount of main memory storage allocated to the program at any one time. Paging, in virtual storage systems, is the process of transferring pages between real storage and external page storage. If a page is not transferred from auxiliary storage until it is actually needed, then paging is said to be done by demand.

parity – A method used by most of the computer industry to determine if data communications hardware has correctly sent and received data characters. All characters are specified as having either an even number of bits (even parity) or an odd number of bits (odd parity).

parity bit – A bit (binary digit) appended to an array of bits to make the sum of all the "1" bits in array either always even (even parity) or always odd (odd parity).

parity check – A check that tests whether the number of "1" bits in an array is even (even parity check) or

odd (odd parity check). See also *row parity check*.

pass – One complete cycle in the execution of a computer program: input, processing, and output. For example, a one-pass compiler reads the source program, compiles it and writes the object program without intermediate input/output operations or human intervention.

password – A unique word or string of characters that a program, computer operator, or user must supply to satisfy security requirements, before gaining access to the system or data.

password protect – A programmed procedure that requires use of a code or access word in addition to normal open file or execute statements.

patching – Correcting or modifying a program in a rough or expedient way by adding new sections of coding. Too many patches in a program make it difficult to maintain. It may also refer to changing the actual machine code when it is inconvenient to recompile the source program.

peer-to-peer communications – Communications in which both sides have equal responsibility for initiating, maintaining, and terminating the session. Contrast with master-slave communications, in which the host determines which users can initiate which sessions. If the host were programmed to allow all users to initiate all sessions, it would look like a peer-to-peer network to the user.

peer-to-peer network – A communications network that allows all workstations and computers in the network to act as servers to all other users on the network. Dedicated file servers may be used, but are not required as in a client/server network.

peripheral equipment – The input/output units and auxiliary storage units of a computer system. (Note: The CPU and its associated storage and control units are the only parts of a computer system that are not considered peripheral equipment.)

physical layer – defines the mechanical, electrical, and procedural characteristics needed to establish, maintain, and release a physical connection. Examples of protocols at this level include RS232 and RS449.

point-to-point – Data flows between two points in a network.

polling – A teleprocessing procedure in which the telecommunications control unit determines if a terminal is ready to send or receive a message. When a computer polls, it asks each terminal in a predefined sequence whether it has any data to transmit. If the terminal has nothing to send it goes to the next terminal (node) in sequence. If a computer has something to send it temporarily suspends polling to receive the data, then resumes polling after the transmission is sent.

POS (Point Of Sale) – A system of terminals that debits a customer's account and credits a merchant's account to effect payment for purchases at retail establishments. For example, an authorized purchase usually causes a real-time debit entry to be made in the purchaser's account with a simultaneous credit entry in the merchant's account. These entries are recorded, not by paper, but by electronic signals flowing between the POS terminals and the respective accounts involved.

positive verification – A method of direct verification that requires a response from the customer. See *direct verification*.

post – Recording onto detailed subsidiary records (ledgers) amounts that have been originally recorded in records of original entry, such as deposit tickets, withdrawal slips, checks, debit or credit memoranda, blotters or journals.

post edit – To edit output data from a previous computation.

post-mortem routine – A diagnostic routine, often a dump, that is used after a program has failed to operate as intended.

PPP (Point-to-Point Protocol) – A protocol that allows a computer to connect to the Internet through a dial-in connection and enjoy most of the benefits of a direct connection, including the ability to run graphical front ends such as Mosaic and Netscape Navigator. PPP is generally considered to be superior to SLIP, because it features error detection, data compression, and other elements of modern communications protocols that SLIP lacks. Contrast with SLIP.

pre-edit – To edit input data prior to computation.

presentation layer – Transforms data from real terminal devices or application data generators into a standard terminal data stream. This layer also handles message compression and encryption.

preventive maintenance – Maintenance carried out to keep equipment in proper operating condition and to prevent faults from occurring during subsequent operations. A maintenance plan that is designed to prevent failures rather than correct malfunctions.

print server – A computer whose primary responsibility is to allow users to share a printer or printers. Documents to be printed are sent to a queue on the print server that then directs the job to the appropriate printer.

privilege – A special authorization that is granted to particular users to perform security relevant operations.

program – A sequenced set of instructions to a computer to do a particular job.

program compatibility – A characteristic enabling one computer system to execute programs written for another computer system and to obtain identical results. Note: Program compatibility can be achieved between two computer systems with similar instruction repertoires and facilities, or by the use of emulators, simulators, translators, or coding in a common language, between dissimilar computers.

program flowchart – A flowchart diagramming the processing steps and logic of a computer program. Contrast with system flowchart.

program listing – A printout, usually prepared by a language translation, that lists the source language statements of a program.

program check – A check that is carried out by a series of instructions in a program.

programmer – A person who devises and writes programs in coding instructions such as COBOL. (Note: The term "programmer" is most suitably applied to a person who is mainly involved in formulating programs, particularly at the level of flowchart preparation. A person mainly involved in

the definition of problems is called an analyst, and a person mainly involved in converting programs into program code suitable for entry into a computer system is called a coder. In many organizations, all three of these functions are performed by programmers.)

programming – Preparing a list of instructions for the computer to use in solving a problem.

proof machine – A machine with multiple pockets that is designed to balance and encode debit and credit transactions, accumulate pocket and grand totals and sort the source documents according to their type (see batch proof). Single pocket proof machines prove the debits and credits of each transaction to itself and do not sort the source documents. This is generally done on high speed MICR reader/sorter equipment (see reader/sorter).

proof-of-deposit (POD) – A method that encodes items with machine-readable dollar amounts. The debits and credits are proven for each transaction and control totals are accumulated for use in subsequent processing.

protocol – A standardized set of rules that specify the format, timing, sequencing and/or error checking for data transmissions. A set of rules that define how computers communicate with each other.

prototyping – A methodology for building a model of what a finished system will look like without completing all stages of the systems development life cycle (SDLC). Prototyping often uses a 4GL language to develop prototype systems.

Q

query language – In data base management systems, a generalized language that allows a user to select records from a database. Query by example (QBE) and structured query language (SQL, pronounced sequel) are examples.

queuing – Method of providing for execution of jobs in a specific order, often according to priorities.

QTAM (Queued Telecommunications Access Method) – An extension of BTAM that includes all of the BTAM facilities but will not support synchronous communications. QTAM provides macro language for the control and processing of communication information including message editing, queuing, routing, and logging. It can schedule and allocate facilities, poll terminals, perform error checking routines, reroute messages, cancel messages, etc. QTAM is not used much because it has been replaced by TCAM.

R

raised check – A check on which the amount has been illegally increased. To deter checks from being raised, they are designed so that the amount is clearly shown in two places: 1) the amount of the check is written in numerical figures near the right margin and after the payees name; and 2) the check amount is either spelled out or protected by machine printing or perforation below the payees name.

RAM (Random Access Memory) – The generic term for read/write memory, memory that permits bits and bytes to be written to it as well as read from it, in any order or sequence. This type of memory is used for temporary information storage. Access to and from RAM memory is very fast. RAM requires electrical power to remember. Information in RAM is lost when the power is turned off.

random access – Pertaining to a storage device whose access time is not significantly affected by the location of the data to be accessed. (Note: Any item of data stored on-line can be accessed within a relatively short time (usually less than one second).) See direct access. Contrast with *serial access*.

raw data – Data that has not been processed or converted to machine-readable form.

reader/sorter – A high speed document handler that reads the MICR encoded information on documents for transmission to a computer and sorts the MICR documents on digits selected either at the unit console (off-line) or by the computer program (on-line).

real storage – In virtual storage systems, the storage of a computing system from which the central processing unit can directly obtain instructions and

data, and to which it can directly return results.

real-time – The processing of transactions on the computer as they occur rather than batching them for processing at a later time.

recap – An abbreviated term for recapitulation (or assembling) of totals for final bank settlement. All totals taken from batch proof sheets or from proof machines must be assembled in proper order so as to build up control totals for various departments charged with the items. Recap sheets may be used in all departments of the financial institution. All recap sheets are assembled into a final recap sheet for settlement of the entire financial institution.

reconcile – A process of accounting for the difference in two records by properly accounting for each outstanding item that, if posted, would bring the two records into agreement.

record – A collection of related data items. Note: In payroll processing, for example, an employee's pay rate forms a field, a set of all fields relating to a particular employee forms a record and a complete set of employee records forms a file. See also *fixed-length record* and *variable-length record*.

record count – A count of the number of records in a file or the number of records processed by a program. Note: Such a count is used in error control to detect the nonprocessing of records.

record gap – Same as *interblock gap*.

record layout – A diagram showing the size, position, and composition of data items making up a record. Note: Such a diagram is prepared during the preparation of a program.

record mark – A special character used in some computers either to limit the number of characters in a data transfer operation or to separate block records on tape.

redundancy check – A check based on the transfer of more bits or characters than the minimum number required to express the message itself; the added bits or characters have been inserted systematically for checking purposes. (Note: The most common type of redundancy check is a parity check.)

re-engineering – A process involving the extraction of components from existing systems and restructuring these components to develop new systems or to enhance the efficiency of existing systems. Existing software systems thus can be modernized to prolong their functionality. An example of this is a software code translator that can take an existing hierarchical data base system and transpose it to a relational data base system. CASE includes a source code re-engineering feature.

regeneration – The restoration of stored information.

relocate – In programming, to move a routine from one portion of internal storage to another and to automatically adjust the necessary address references so that the routine, in its new location, can be executed.

report file – A file containing transactions records and/or results of a data processing job.

report generation – A technique for producing complete machine reports from information that describes the input file and the format and content of the output report.

rerun – To make another attempt to complete a job by executing all or part of the process again with the same or corrected inputs.

rerun point – A point in a program where its execution can be re-established after an equipment failure or some other interruption. Note: Sufficient data is recorded at a rerun point to permit a restart from that point in the event of a subsequent interruption. Thus, the provision of rerun points at reasonable intervals can save computer time by making it unnecessary to rerun a program from the beginning whenever a run is interrupted.

resource – Any part of a computing system or operating system required by a job or task, including main storage, input/output devices, processing unit, data sets, and control or processing programs.

restart capability – Ability to reestablish the execution of a program whose execution has been interrupted by using restart points.

Rewritable (erasable disks) – are three and a half and five and one quarter inches in size. They are contained in cartridges and can be created (written to)

and then changed (erased) by users. Common technology for rewritable disks is magneto-optic technology. Such disks are used for documents that are frequently changed and updated.

ring topology – A network topology in which nodes are connected to a closed loop. Terminators are not required because there are no unconnected ends.

RISC (Reduced Instruction-Set Computer/Computing) – A computer architecture that reduces chip complexity by using simpler instructions. RISC compilers have to generate software routines to perform complex instructions that were previously done in hardware by CISC computers. The RISC chip is faster than its CISC counterpart and is designed and built more economically. Contrast with CISC.

RJE (Remote Job Entry) – Input of a batch job from a remote site and receipt of output via a line printer at a remote site. The technique allows various systems to share the resources of a batch oriented computer by giving the user access to centrally located data files and to the power necessary to process those files.

ROM (Read Only Memory) – A computer memory that stores permanent information. This information is constant and cannot be erased, or changed, or lost, even if electrical power is turned off. All PCs contain programs in ROM that execute when the power is turned on (*BIOS*).

router – A computer system in a network that stores and forwards data packets between LANs and WANs. Routers see the network as network addresses and all the possible paths between them. They read the network address in a transmitted message and can make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.) Because routers have to inspect the network address in the protocol, they do more processing than a bridge and add overhead to the network.

routine – A set of instructions arranged in correct sequence that causes a computer to perform a particular process. Note: In this context, the term, routine is somewhat more precise than the general (and more commonly used) term program.

row – A horizontal arrangement of characters. See *frame*.

row parity check – A parity check performed on the bits in each row of a magnetic tape or punched tape. Synonymous with *lateral parity check*.

RPG (Report Program Generator) – A generator designed to construct programs that perform routine report-writing functions, such as programs that accept input data from magnetic tape or disk files and produce printed reports, often with headings and subtotals.

run – The single and continuous execution of a program by a computer using a given set of data.

run manual – A manual documenting the processing system and operating instructions associated with a computer run.

S

secondary storage – Synonymous with *auxiliary storage*.

security administrator – The person or group that has responsibility for the administration and management of the security mechanism.

security audit trail – Data collected and used to facilitate a security audit. A set of records that collectively provides documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, or backwards from records and reports to their component source transactions.

security mechanism – The technological and managerial safeguards established and applied to a data processing system to protect hardware, software, and data from accidental or malicious modifications, destruction, or disclosure.

security relevant event – Any event that attempts to change the security state of the system, such as change discretionary access controls, change the security level of the subject, change user password, etc. Also, any event that attempts to violate the security policy of the system, such as too many invalid attempts to logon, attempts to violate the

mandatory access control limits of a device, attempts to downgrade a file, etc.

selective dump – A dump of the contents of a set of storage locations specified by the user; for example, a dump of the storage locations occupied by a particular program or its data.

selector channel – A high-speed channel capable of one-way transmission. Selector channels operate in burst mode.

self-checking code – Same as *error-detecting code*.

self-checking number – An account number that contains redundant information (such as an appended check digit) permitting it to be checked for accuracy after it has been transferred from one medium or device to another. See *check digit*.

sense switch – A hardware switch on some types of computers that can be set by an operator and whose position can be sensed by a program instruction. Note: Such a switch can be used for programs that have alternate processing paths selected by the operator through the switch setting. A sense switch also may be a logical switch provided by the programmer to detect specific conditions.

sentinel – A character or symbol that signals a particular condition, such as the end of a file.

sequencing – The process of dividing a user data message into smaller frames, blocks, or packets for transmission, where each has an integral sequence number for reassembly of the complete message at the destination end.

sequence test – A process of checking the validity of the order in a series or rank or time.

sequential – In numeric sequence, normally in ascending order.

sequential processing – Processing from low order to high order in serial sequence.

serial access – Pertaining to a storage device in which there is a sequential relationship between the access times to successive location, as in the case of magnetic tape. Contrast with random access.

server – is one or more multi-user computer (back-end), usually a mainframe or a minicomputer, although it could be a PC. Server functions include any centrally supported role, such as file sharing, printer sharing, database access and management, communication services, facsimile services, application development, and others. Multiple functions may be supported by a single server.

session layer – performs bind/unbind processing; determines many characteristics of how the dialog between applications proceeds.

shareware – Computer programs from Electronic Bulletin Boards (EBBs) or other public sources for which developers ask the user to send money for registration, recompense, manuals, etc.

service charge – A fee charged by a bank for services rendered to a customer.

simplex channel – A channel that permits transmission in one direction only.

simulator – A software routine that is executed by one computer but imitates the operations of another.

slide – A term used in bookkeeping to describe a posting error by which an amount is wrongly recorded as a result of the bookkeeper unintentionally placing the decimal one or more digits to the right or left of the true decimal position. Example: posting \$5.03 as \$50.30, or as \$503.00.

SLIP (Serial Line Internet Protocol) – A protocol that allows a computer to connect to the Internet through a dial-in connection and receive most of the benefits of a direct connection, including the ability to run graphical front ends such as Mosaic and Netscape Navigator. SLIP is also used to run TCP/IP over phone lines. Contrast with PPP. See also *TCP/IP*.

smart card – A device the approximate size of a credit card that contains an embedded microprocessor for storing information about an individual.

smart terminal – See terminal.

SNA (Systems Network Architecture) – IBM's mainframe network standards, introduced in 1974. Generically, the term refers to the description of the logical structure, formats, protocols, and operational

sequences for transmitting information units through, and controlling the configuration and operation of, networks.

snapshot – A dynamic dump of the contents of specified storage locations and/or register that is performed at specified points or times during running of a program.

software – A collection of programs (stored sets of instructions) that govern the operation of a computer system and makes the hardware run. Contrast with hardware.

sort – To arrange items in sequence or to segregate items into groups according to an aspect of their keys or certain rules. Note: Often keys are groups of numbers or letters, such as account numbers or employee names, and the sorting operation involves arranging the items so that keys of successive items are in numerical or alphabetical sequence. Sorting is one of the most common data processing operations.

source document – A document from which data is extracted and entered into a computer system; for example, a document that contains typed or handwritten data for data entry.

source language – A language that is an input to a translation process or in which a program is written. Contrast with *object language*.

source program – A computer program written in source language (for example, a program written in COBOL) or symbolic language that will be converted into an absolute language object program using a processor program.

spoofing – An attempt to gain access to a system by posing as an authorized user.

SPOOL (Simultaneous Peripheral Operation On-Line) – An application that manages print requests or jobs so that one job can be processed while other jobs are placed in a queue (an ordered list of items waiting to be processed) until the printer has finished with preceding jobs. Also called *print spooler*.

spooler – A program that intercepts data going to a device driver and writes it to disk. The data is later processed when the device is available. A spooler prevents output from different sources from being

intermixed.

spooling – The process of temporarily storing print jobs while waiting for an available printer or port. Spooling jobs (tasks) frees system resources from waiting for a relatively slow device to provide output and keeps the contents of each print job separated from the contents of every other print job. Output to slow devices are put in "a waiting line" on mass storage devices to await transmission. In this way, more efficient use of the system is allowed since programs using low-speed devices can run to completion quickly and make room for others.

SQL (Structured Query Language) – Pronounced "sequel." A query language developed by IBM that relies on simple English-language statements to perform database queries. Almost universally supported in one form or another by relational databases on platforms of all types, SQL allows databases from different manufacturers and on different types of computers to be queried using a standard syntax.

star topology – A network topology in which nodes are connected to a common device such as a hub or concentrator.

statement of account – A record prepared by a financial institution for the customer that details the activity and balance within the customer's account(s). The statement of account is usually accompanied by the deposit slips and canceled checks that correspond to the detailed activity.

statement of condition – A detailed listing of a financial institution's resources, liabilities and capital accounts showing its condition on a given date. On request (calls by state and/or federal supervisory authorities several times a year), financial institution's are required to submit sworn statements of condition. In general accounting, this type of financial report is known as a balance sheet and is actually a trial balance of all general ledger accounts. This record is also termed the Daily Statement of Condition.

steering committee – A management committee that establishes goals and objectives for the information systems (IS) and data processing function and allocates resources. Also monitors performance of the function through management reports.

storage – A device or portion of a device that is capable of receiving data, retaining it for an indefinite period of time, and supplying it on command.

storage dump – Same as *dump*.

storage protection – Protection against unauthorized writing in or reading from all or part of a storage device. Note: This protection may be implemented by using manually set switches or automatic hardware facilities, usually in connection with an operating system. Effective storage protection is vital in multi-programming and time-sharing systems both for ensuring privacy and for preventing concurrently operating programs from interfering with one another.

string – A connected sequence of characters, words, or other elements.

subroutine – Program segments that perform a specific function at any time in the program, thereby reducing programming and debugging labor.

supervisory state – One of the two general states in which a computer system executes instructions, the other being user state. Certain privileged instructions can be executed in the supervisor state that may bypass security mechanisms.

summation check – A check in which the sum of a group of digits is formed (usually without regard to overflow) and compared to a previously computed value called the checksum.

supervisor – Part of the operating system that organizes and regulates the flow of work in a computer system by initiating and controlling execution of programs.

supervisory routine – Same as *executive routine*.

support software – Programs that aid computer operations or programming or are an adjunct to application software. Examples of such software include: job accounting systems, automated tape library and scheduling systems, software librarian systems, and software providing access control over a telecommunications network.

surge protector – An inexpensive electrical device that prevents high voltage surges from reaching a computer and damaging its circuitry. See *UPS*.

symbolic address – An address that is expressed in symbols convenient for the programmer, but that must be translated, usually by an assembler, into absolute symbols before it can be interpreted by a computer.

symbolic coding – Coding that uses machine instructions with symbolic addresses. Note: The input to most assemblers is expressed in symbolic coding. Mnemonic operation codes are usually employed in addition to symbolic addresses to further simplify the coding process. A two-address instruction that subtracts an employee's taxes from his or her gross pay, for example, might be written SUB TAX GPAY. Contrast with *absolute coding*.

synchronization check – A hardware check that determines whether a particular event or condition occurs at the correct moment; for instance, whether the print hammers in a drum printer are activated at the moment when the appropriate character slugs on the drum are in correct position.

synchronous communications – A method of data communication in which the transmission of bits of data is synchronized by a clock signal. It requires the use of constant time intervals between events or occurrences when transmitting data. Synchronous communications sends data in parallel along a bus with each wire corresponding to one bit of information in a binary number. Start and stop bits are not required. Synchronous communication can be compared to sending eight cars side-by-side down a freeway. The cars travel together, and they arrive at the same time.

Synchronous Optical Network (SONET) – A standard being developed by the National Exchange Carriers Association. This is a standard for optical transmissions at a high rate of speed, usually in gigabits per second speeds.

system – A set (or arrangement) of components that form an organized whole. Note: This term is general and is applied to both hardware and software elements. Therefore, it is meaningful only when carefully qualified - for example, computer system, management information system, operating system.

system administrator – The person at a computer installation who is responsible for installing and maintaining system software.

system activity log – A system-generated report that details all communications between the operator and the system and between different parts of the system. The log also details all jobs run and files used.

system analysis – Examination of an activity, procedure, method, technique or business to determine what changes should be made and how they should be accomplished.

systems analyst – An individual who defines the application problem, determines system specifications, recommends equipment changes, and designs data processing procedures. This person also devises data verification methods and prepares block diagrams and records layouts from which the programmer prepares flowcharts and codes the programs. May assist in or supervise the preparation of flowcharts.

system configuration – (1) A specific set of equipment units interconnected and programmed to operate as a system; (2) the rules concerning the interconnection of available equipment units that collectively define the range of possible configurations in a particular computer system.

system design – The specification of the working relationships between all parts of a system in terms of their characteristic actions.

Systems Development Life Cycle (SDLC) – The stages through which software evolves from an idea to implementation. Although the names of the stages may vary, they usually are: feasibility, design (functional specifications, technical specifications), development (programming, testing), and implementation. These phases may vary depending on the complexity of the system being developed.

Systems Development Life Cycle Methodology (SDLCM) – The tasks, processes and deliverables associated with successfully completing each of the phases or stages associated with a system development project and documenting them.

system flowchart – A flowchart diagramming the flow of work, documents, and operations in a data processing application.

system library – A collection of data sets in which various parts of an operating system are stored.

system log – Report in which job-related information, operational data, descriptions of unusual occurrences, commands and messages to or from the operator are listed.

systems programmer – A programmer who plans, maintains, extends and controls use of an operating system to improve the overall productivity of an installation.

system utility programs – Programs supplied by the manufacturer to perform routine or special tasks. These programs are supplied as part of the manufacturers' software package.

T

tag – One or more characters attached to a particular item or record and used to identify that item or record. Note: The tag may be removed from the item or record by a simple operation, but it then loses its significance. Contrast with *key*.

TCAM (Telecommunications Access Method) – IBM communications software widely used to transfer data between mainframes and 3270 terminals. Contrast with *BTAM* and *QTAM*.

TCP/IP (Transmission Control Protocol/Internet Protocol) – A communications protocol developed for the U.S. Department of Defense to interconnect dissimilar systems. It is a de facto UNIX standard, but is supported on almost all computer systems. TCP/IP is the protocol of the Internet. TCP controls data transfer. IP provides the routing.

TCU (Telecommunications Control Unit) – A physical device that controls the terminal's activities and acts as an interface between the terminals and the central processor.

technical support group – Oversees systems development and serves as liaison between programming and IS operations. Usually consists of several systems programmers with high-level technical knowledge.

telecommunications – Data transmission between computing system and remotely located devices via telephone lines or microwave transmissions.

teller proof – A system of individual teller control where the teller balances and settles his or her own cash position daily. Teller proof consists of using the teller's starting cash total, adding his or her cash received, and subtracting his or her cash paid out, to arrive at cash on hand. The cash counted must agree with the ending cash total.

teleprocessing – The processing of data that is received from or sent to remote locations by way of telecommunications.

terminal – A keyboard/display or keyboard/printer device used to input programs and data into the computer and to receive output from the computer. A dumb terminal has no processing capability. A smart, or intelligent, terminal has some processing capability and, in some cases, a disk drive so that information can be downloaded.

test data generator – Software aid used for forming test data files by holding desired or randomly generated values in nominated fields of nominated records. Most effective if controlled by the record data definitions used in application programs so that fields can be identified by the same symbolic names, and test data can be recompiled in the same manner as programs, upon a change of field or record format.

test routine – A routine designed to test whether a computer is operating correctly.

third-party maintenance – Refers to various field engineering companies that offer contract maintenance and operation of computers not owned or leased by them for charges and fees commensurate with the system's size and complexity.

throughput – The total amount of useful work performed by a data processing system during a given period of time.

time-sharing – A method of operation in which the resources of a computer facility are shared by users via terminals for different purposes at (apparently) the same time. Although the computer actually services each user in sequence, the high speed of the computer makes it appear that users are all handled simultaneously. The user and the computer usually communicate by way of a higher level, easy-to-learn computer language.

topology – The arrangement of nodes usually forming a star, ring, tree, or bus pattern. Also called network topology.

trace routine – A diagnostic routine designed to check or demonstrate the operation of a program. Note: The output of such a routine usually includes some or all of the instructions (and their immediate results) in the program being checked, arranged in the sequence in which they are executed.

track – The part of a data storage medium that influences or is influenced by one head. For example, the ring-shaped portion of the surface of a drum associated with one nonmovable head or one of several (most commonly 7 or 9) divisions running parallel to the edges of a magnetic tape.

track parity check – Same as *longitudinal parity check*.

trailer record – A record that follows another record or group of records and contains data pertinent to the record or group of records.

transaction code – One or more characters that form part of a record and signify the type of transaction represented by that record. In inventory control, for example, a transaction code may signify deliveries to stock, disbursements from stock, order, etc.

transaction file – Same as *detail file*.

transit department – A department of a financial institution that processes checks drawn on other institutions (e.g., out-of-city or not-on-us items). The transit department prepares all transit check clearing letters and forwards these letters to the Federal Reserve bank, correspondent financial institutions, etc., for collection and payment.

transit items – Cash items that are drawn on financial institutions outside the immediate exchange or local forwarded clearinghouse area. These items are then processed and forwarded to Federal Reserve banks, correspondent financial institutions, etc., for collection and remittance to the financial institution that originally received the items.

transit letter – A deposit form or remittance instruction slip that describes and gives totals of items to be collected and paid, enclosed with checks

and other cash items. The term cash letter refers to transit items sent to a financial institution where the remitting institution maintains an account. A remittance letter is sent when payment must be made (usually by draft) for the items sent.

translator – A device or computer program that performs translations from one language or code to another; for example, an assembler or compiler.

transmission – Data is transmitted in one of three modes: Simplex, Half-Duplex, and Full-Duplex.

- Simplex – Data transmission occurs in one direction only.
- Half-Duplex – Transmission occurs in two directions but only in one direction at a time.
- Full-Duplex – Transmission occurs in both directions simultaneously.

transport layer – provides transparent transfer of data between sessions entities. This layer segments messages if necessary and implements flow control.

transposition – The unintentional reversal of two digits in a number.

trap – An unprogrammed jump to a particular location, activated automatically upon the occurrence of a particular condition. This may occur, for example, upon an attempt to execute an instruction that is not in the computer's instruction repertoire. Note: The point where the jump occurs is recorded, so that normal execution of the program can be resumed after the faulty condition has been corrected.

trapdoor – A concealed and unauthorized entrance into a computer operating system. The programmer who designs and installs the trapdoor would have the opportunity to enter a system, take control of it, and by-pass any standard safeguards installed for audit control purposes.

tree topology – A network topology in which nodes are connected by cables to a trunk cable with a central retransmission facility.

trial balance – Listing the balances of all accounts within a given control or ledger and proofing it to the control total established over the group of accounts

affected. Trial balances of bookkeeping department ledgers are usually taken at least once a month. The daily statement of condition (see definition) is, in effect, a daily trial balance of the general ledger.

troubleshoot – Same as *debug*.

TSR (Terminate-and-Stay-Resident) – A memory resident program that remains active in memory when other programs are running. It is not visible until you press a certain key combination or until a certain event occurs. A typical example is a screen saver program that will activate after a certain time period, or if the user presses a certain key combination. Also called memory resident or pop-up program.

turnaround – The time elapsed between submission of a job to a computer center and when results are returned.

twisted pair cable – A wiring scheme with one or more pairs of 18 to 24 gauge copper strands. The strands are twisted to improve protection against electromagnetic and radio frequency interference. Cable may be either shielded or unshielded.

U

uncollected funds – The portion of a deposit or deposit account that has not been collected or paid because the items deposited are en route to the drawee financial institution for payment. Checks drawn against uncollected funds will not usually be paid by a financial institution until it knows that the deposit account is fully available and that all deposits are fully collected. See also *kite*.

update – Pertains to a procedure used to modify a master file with current information.

UPS (Uninterruptible Power Supply) – Backup power used when the electrical power fails or drops to an unacceptable voltage level. Small UPS systems provide battery power for a few minutes; enough to power down the computer in an orderly manner. Sophisticated systems are tied to electrical generators that can provide power for days. A surge protector filters out surges and spikes, and a voltage regulator maintains uniform voltage during a brownout, but a UPS keeps a computer running when there is no

electrical power. UPS systems typically provide surge suppression and also may provide voltage regulation.

UPPER CASE – A term to describe CASE software that automates early stages of software development (planning, design, and analysis). These tools are newer and not as prevalent as lower case tools or traditional programmer productivity aids.

user manual – Written instructions documenting the responsibilities and procedures to be followed in processing data and transactions on the computer system for an individual department or user area.

user – In information security, the entity, human or machine, that is identified by the logon ID, authenticated prior to system access, the subject of all access control decisions, and held accountable via the audit reporting system.

utility program – A specialized program that assists in the operation of a computer by performing a frequently required process, such as sorting, merging, report program generation, data transcription and file maintenance. Note: Utility programs are usually supplied by the equipment manufacturer.

V

validity check – A hardware check that determines whether or not a particular character is a legitimate member of the permissible character set.

variable-length record – A record that may contain a variable number of characters. Contrast with fixed-length record.

vendor – A company that supplies resources and materials, e.g., computer equipment, software packages.

verify – To determine whether a data transcription or data transfer operation is accomplished accurately.

virtual storage – Process by which a program is divided into segments called pages. Only the segment actually being executed will be resident in core at any given time; the balance of the program is stored on a direct-access medium to be used as needed.

virtual address – The immediate address or real-time address.

virus – A computer program that embeds itself in other code and can replicate itself. Once active, it takes unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programs.

VM (Virtual Machine) – An IBM mainframe operating system, originally developed by its customers and eventually adopted as an IBM system product (VM/SP). It can run multiple operating systems within the computer at the same time, each one running its own programs.

VSE (Disk Operating System/Virtual Storage Extended) – An IBM multiuser, multitasking operating system that typically runs on IBM's 43xx series. It used to be called DOS, but due to the abundance of DOS PCs, it is now referred to as VSE.

VTAM (Virtual Telecommunications Access Method) Also called ACF/VTAM (Advanced Communications Function/VTAM), software that controls communications in an IBM SNA environment. It usually resides in the mainframe under MVS or VM, but may be off-loaded into a front-end processor that is tightly coupled to the mainframe. It supports a wide variety of network protocols.

volume – A tape or a disk used for data storage. A file may include one or several volumes. See *file*.

W

WAN (Wide Area Network) – A communications network that covers a wide geographic area, such as state or country, using high speed long distance lines or satellites provided by a common carrier. A LAN (local area network) is contained within a building or complex, and a MAN (metropolitan area network) generally covers a city or suburb. See *LAN* for detail.

wideband – Generally, a communications channel offering a transmission bandwidth greater than a voice-grade channel; data transmission speeds on wideband facilities are typically in excess of 9.6 kbit/s and often at rates of 56 kbit/s and 1.544 Mbit/s.

window – An unauthorized entrance into a computer operating system. See *trapdoor*.

word – A group of bits or bytes treated as a unit and capable of being stored in one storage location.

working storage – A computer storage area set aside by a programmer for various uses including developing processing results, storing constants, and temporarily storing results needed later in the program sequence.

WORM (Write Once, Read Many) disk – A type of disk used extensively in records management applications. The disks are in four sizes (three and a half; five and a quarter; 12 and 14 inches). The disks are blank when purchased, and are written to by users with appropriate hardware and software. Once information is incorporated into a WORM disk with

a laser, it cannot be altered or erased. However, authorized employees can add to the document, and the system can be programmed to explain what was added to the document. The WORM disks can be read thousands of times without deteriorating.

WWW (World Wide Web) – A collection of richly formatted hypertext “pages” located on computers around the world and logically linked together by the Internet. With a graphical Web browser such as Mosaic or Netscape Navigator, users can “surf” the Web by clicking highlighted words on the screen. Each click activates a hypertext link, connecting the user to another Web location.

WYSIWYG (What You See Is What You Get) – Pronounced wissywig or wizzywig. Refers to the ability to display a close representation of the printed page on the computer screen.