Federal
Financial
Institutions
Examination
Council

Information Systems

VOLUME 1

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

Federal Financial Institutions Examination Council

FFIEC Information Systems Examination Handbook

Volume 1

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

FFIEC INFORMATION SYSTEMS (IS) EXAMINATION HANDBOOK SUMMARY OF SIGNIFICANT CHANGES 1996

Most 1996 FFIEC IS Examination Handbook sections have been revised to reflect the rapidly changing information systems environment we supervise. Significant changes include:

- Inclusion of a General/Administrative Section.
- Development of several new narrative chapters and related workprograms.
- Additional guidance on IS supervision by risk.
- Revision of obsolete sections to make the Handbook more relevant and effective as a:
  - Tool for supervision and examination guidance.
  - Reference source for the industry.
  - Training aid for new IS examiners.
  - Technical reference source.
- Positioning each workprogram to follow the narrative section it supports.
- Use of the newer term *information systems* (IS), instead of electronic data processing (EDP).

The 1996 Handbook has been expanded significantly compared with prior biannual releases that began in 1990. The numerous changes and modifications do not represent a policy change for the FFIEC or its member agencies. Rather, they indicate a major reorganization, clarification, and summation, of how IS field examinations have evolved over recent years. This Handbook also addresses new technology pertinent to IS safety and soundness issues. The 1996 Handbook is printed as a two-volume set. Volume 1 includes Sections I and II and describes the purpose of IS examinations, the internal control structures and the workprogram, steps for each IS examination or review. Volume 2 includes Sections III and IV which present the, reference material supporting the FFIEC IS supervisory/examination process.

1996 Handbook revisions include:

Section I – General and Administrative (Chapters 1-7) – VOLUME 1

- Emphasizing the use of FFIEC IS Supervision by Risk (Chapter 2) as the basis for the supervisory approach for IS supervision and examination. This is an evolving policy area for all financial regulatory agencies. The chapter is presented as guidance only and will be supplemented by individual agency policies. The use of a risk-based philosophy will align the approach of the IS examining staffs of several FFIEC member agencies more closely with the direction being taken in their other regulatory examination processes. A key underlying element of the risk-based examining approach is to ensure that supervision resources are applied appropriately to areas where they are most effective. IS examiners will continue to apply examination only resources to identified risk areas and complete appropriate IS workprograms.

- Introducing in three new chapters administrative processes shared by member agencies. The Handbook provides guidance on common approaches and procedures used by member agencies for**:**

  - Examination Planning (Chapter 3).
  - Examination Techniques (Chapter 4).
  - Composite IS Ratings and Reports of Examination (Chapter 5).

  These topics cover the preliminary work (planning); the on-site work (examining techniques); and the conclusionary and follow-up work (IS rating and final IS ROE).

  These activities are common to FFIEC member agencies and are provided as guidance to both IS examiners and the industry.

- Addressing in two new chapters in the General Section the following national programs that fall under the FFIEC's IS Interagency responsibility and direction:

  - MDPS [Multiregional Data Processing Servicers] (Chapter 6).
  - SASR [Shared Application Software review] (Chapter 7).

Section II – Supervisory Tools (Chapters 8 - 23) – VOLUME 1

Supervisory Tools contains several new narrative chapters and related workprograms. They address newer areas of technology reviewed by examiners. Several sections also have been revised to provide a clearer focus on the need for, and review of, internal controls within the IS supervision of financial institutions and servicer data centers. These Handbook changes include:

- Expansion of the Management area (Chapter 9), including an introduction to the Internet and some of the potential issues it raises for the industry and its regulators [Emerging Technology section].

- Consolidation of information from several of the Operations related chapters in Corporate Contingency Planning (Chapter 10).

- Placement of information on enterprise-wide or corporate disaster/recovery and contingency planning concerns as a part of the overall senior management review. This placement reflects more accurately interagency emphasis on this area as a senior management responsibility.

- Placement of MIS Review (Chapter 11), under the umbrella of management to re-enforce the overall importance of management information systems to both the strategic and tactical decision activities of the institutions, whether financial or commercial.

- Expansion of Networking and Client/Server (Chapter 15) and End-User Computing (Chapter 16) to include a new section on Client/Server (C/S) Technology issues and basic controls that should be considered in a C/S processing environment.

- Addition of Document Imaging (Chapter 17) related controls expands supervisory review to the risks and issues surrounding financial institution document imaging technology.

- Development of four distinct chapters that review EFT (electronic funds transfer) and correlate closely to the various types of EFT activities performed and reviewed by examiners, including the following chapters that address:

  Wholesale EFT – Traditional com-mercial/large dollar wire transfer activity and a new discussion related to the money laundering issue and related control and regulatory considerations (Chapter 18).

Fedline EFT – Internal controls surrounding the PC front-end to the Fedwire network [used by smaller institutions to effect traditional commercial EFT activities] (Chapter 19).

Retail EFT – The areas of ATMs, POS, debit cards, smart cards, home banking, etc. (Chapter 20).

ACH – Risks and controls basic to automated clearinghouse operations provided by both financial and commercial institutions (Chapter 21).

- Expansion of IS Servicing Provider/Receiver (Chapter 22) and Community Financial Institution IS Examination Program [formerly called the Turnkey Exam] (Chapter 23). Both are now found at the end of this section. These areas of IS related review previously fell outside the scope of on-site IS examination process and are referenced here to provide direction and guidance in their use at community institutions.

- Placement of each workprogram after the detailed narrative chapter that supports and introduces the internal control concerns for that workprogram.

- Organization of the chapters in a more logical manner. This sequence supports the traditional IS rating component schema of: Audit - Management - Systems Development and Programming - Operations.

Section III – Laws and Policies (Chapters 24 - 30) – VOLUME 2

Section three addresses IS Laws and Policies under which IS supervision has evolved and the current IS related policies of the FFIEC and each of its member agencies (Chapters 24 - 30).

Section IV – Other References and Tools – VOLUME 2

This final section of the Handbook, Other Tools and References, includes:

- An expanded Glossary of terminology used in the areas of microcomputers, client/servers, networking, imaging, and traditional mainframe IS environments.

This revision begun in March 1995 represents the combined efforts of senior IS examiners from the five FFIEC member agencies and the Farm Credit Administration. The 1996 FFIEC IS Examination Handbook (1996 Handbook) is intended to guide IS examiners in conducting examinations and to be a valuable reference source for financial institution and private servicer management and auditors, external auditors, and to the industry.

TABLE OF CONTENTS

VOLUME 1 – Section I GENERAL and ADMINISTRATIVE

Chapter 1 **Introduction** **1-1**
(FFIEC Disk #1 and File Name S1C1.wpd)

Chapter 2 **IS Supervision by Risk** **2-1**
(FFIEC Disk #1 and File Name S1C2.wpd)
FFIEC IS Risk Overview Program **2-1**
Risk Definition **2-1**
Risk Analysis **2-2**
Supervisory Strategies **2-5**

Chapter 2WP **IS Supervision by Risk Workprogram** **2-7**
(FFIEC Disk #3 and File Name IS-WP#01.wpd)

Chapter 3 **Examination Planning** **3-1**
(FFIEC Disk #1 and File Name S1C3.wpd)
IS Examination Types **3-1**
Frequency of IS Examinations **3-1**
Time Standards for IS Examinations **3-2**
Financial Institution Examinations **3-2**
Service Providers' Examinations **3-4**
Gathering Information **3-5**
Scoping the Examination **3-5**
Coordinating the Examination **3-6**
Notification of the Examination **3-6**

Chapter 3WP **Examination Planning Workprogram** **3-9**
(FFIEC Disk #3 and File Name IS-WP#02.wpd)

Chapter 4 **Examination Techniques** **4-1**
(FFIEC Disk #1 and File Name S1C4.wpd)
On-Site Procedures **4-1**
Time and Budget **4-2**
Workpaper Guidelines **4-2**
Workpaper Organization/Format **4-3**
Workpaper Review **4-3**
Conclusions Memos **4-4**
Summary of Conclusions **4-4**
Exit Conference **4-5**
Board Meeting **4-5**
IS ROE Format **4-5**
Service Provider Report Distribution **4-5**
Enforcement Actions **4-6**

Chapter 5 **IS Examination Ratings and ROE** **5-1**
(FFIEC Disk #1 and File Name S1C5.wpd)
Composite Ratings **5-1**

Component Ratings Definitions 5-1
Component Rating Areas of Coverage 5-2
FFIEC IS ROE Introduction 5-4
Guidelines for Completing 5-4
Sections of ROE 5-4
Open Section - Required and Optional Pages 5-5
Administrative Section - Required and Optional Pages 5-6

Chapter 6 **Multiregional Data Processing Servicer (MDPS) Program 6-1**
(FFIEC Disk #1 and File Name S1C6.wpd)
Responsibilities of Lead Agencies 6-1
General Procedures 6-2
Report Preparation and Distribution 6-2

Chapter 7 **Shared Application Software Review (SASR) Program 7-1**
(FFIEC Disk #1 and File Name S1C7.wpd)
SASR Program 7-1
Objectives 7-1
Responsibility 7-1
Administration 7-2
Guidelines for SASR Reports 7-3
Attachments – Sample SASR Forms 7-7

VOLUME 1 – Section II SUPERVISORY TOOLS

Chapter 8 **Internal/External Audit 8-1**
(FFIEC Disk #1 and File Name S2C8.wpd)
External Audit Policy Guidance 8-1
Selecting the Audit Structure 8-1
Role of the Internal Auditor 8-3
Independence and Staffing of Internal IS Audit 8-3
Internal Audit Risk Methodology 8-5
Internal Audit Manual 8-5
Planning, Organizing, and Supervising an IS Audit 8-6
Audit Procedures 8-7
Audit Participation in Application Development/Testing or Acquisition 8-10
Audit Reports and Documentation 8-10
Audit Follow-up 8-11
Role of External Auditor 8-11
Third-party Reviews of Service Centers 8-12
End-user Computing Audit Coverage 8-12
Examining the IS Audit Function 8-14
Legal Requirements - Annual Independent Audits 8-15

Chapter 8WP **Internal/External Audit Workprogram 8-17**
(FFIEC Disk #3 and File Name IS-WP#03.wpd)

Chapter 9 **Management 9-1**
(FFIEC Disk #1 and File Name S2C9.wpd)
Management 9-1
Organization 9-1
Planning 9-6
Controls 9-8
Financial Analysis 9-11
Insurance 9-12

Management Appraisal 9-14
Management Information Systems 9-14
Outsourcing Data Processing Services 9-16
Systems Conversions 9-17
Emerging Technologies 9-18
The Internet 9-19
Client/Server Computing Systems 9-23
Electronic Imaging Systems 9-24
Electronic Data Interchange (EDI) 9-24

Chapter 9WP **Management Workprogram 9-27**
(FFIEC Disk #3 and File Name IS-WP#04.wpd)

Chapter 10 **Corporate Contingency Planning 10-1**
(FFIEC Disk #1 and File Name S2C10.wpd)
Corporate Contingency Planning Responsibilities 10-1
Organizational Planning Guidelines 10-1
Backup and Contingency Planning 10-2
IS Contingency Planning 10-4
Protection against Physical Disasters and other Disruptions 10-4
Hardware Backup 10-6
Program and Software Backup 10-7
Data File Backup 10-8
Telecommunications Backup 10-8
Insurance 10-9

Chapter 10WP **Corporate Contingency Planning Workprogram 10-11**
(FFIEC Disk #3 and File Name IS-WP#05.wpd)

Chapter 11 **Management Information Systems (MIS) Review 11-1**
(FFIEC Disk #1 and File Name S2C11.wpd)
Risks Associated with MIS 11-2
Assessing Vulnerability to MIS Risk 11-2
Achieving Sound MIS 11-3
MIS Reviews 11-4

Chapter 11WP **MIS Review Workprogram 11-5**
(FFIEC Disk #3 and File Name IS-WP#06.wpd)

Chapter 12 **Systems Development and Programming 12-1**
(FFIEC Disk #1 and File Name S2C12.wpd)
Project Control 12-1
Systems Development Standards 12-2
Software Acquisition 12-4
Programming Standards 12-5
Testing Standards 12-6
Systems Implementation 12-6
Software Maintenance 12-7
Integrated Software Systems 12-9
Operating Systems 12-10
Programming Personnel 12-12
Program Security 12-13
Documentation Standards 12-14
Application Software Documentation 12-14
Maintenance of Documentation 12-18

User Manual Documentation 12-22
Purchased Software Documentation 12-22
Data Base Management Systems 12-23
Computer-Aided Software Engineering (CASE) 12-30

Chapter 12WP Systems Development and Programming Workprogram 12-33
(FFIEC Disk #3 and File Name IS-WP#07.wpd)

Chapter 13 Operations 13-1
(FFIEC Disk #1 and File Name S2C13.wpd)
Separation and Rotation of Duties 13-1
Equipment Maintenance 13-2
Equipment Operations 13-3
Scheduling 13-3
Backup 13-4
Equipment Controls 13-5
Operator Controls 13-6
Library Controls 13-6
Control of Data File Media 13-8
Housekeeping 13-10
Emergency Procedures 13-10
Transaction Processing 13-10
Transaction Initiation and Data Entry 13-11
Batch Proof and Balancing Control 13-13
Terminal Entry 13-14
Output Distribution and Control 13-15
Review and Reconcilement of Output 13-16

Chapter 13WP Operations Workprogram 13-19
(FFIEC Disk #3 and File Name IS-WP#08.wpd)

Chapter 14 Security – Physical and Data 14-1
(FFIEC Disk #1 and File Name S2C14.wpd)
Security Administration and Accountability 14-1
Security Plan 14-2
User Education 14-2
Physical, Building, Cabinet, and Vault Security 14-2
Physical Security for PCs and Distributed IS Environments 14-3
Personnel, Data File Media, and Computer Operations Security 14-4
Hardware and Software Inventory 14-5
Data Security 14-6
Logical Access Security and Controls 14-7
Program Security 14-9
Data Integrity 14-10
Telecommunications Security and Access Controls 14-12
Transmission Controls 14-13
Computer Viruses 14-15

Chapter 14WP Security – Physical and Data Workprogram 14-19
(FFIEC Disk #3 and File Name IS-WP#09.wpd)

Chapter 15 **Networking – Client/Server** **15-1**
(FFIEC Disk #2 and File Name S2C15.wpd)
Network Architecture/Components **15-1**
Logical Models **15-2**
Other Protocols and Standards **15-4**
Data Transmission **15-4**
Host Computer Components **15-6**
External Connections **15-6**
Communications Media and Carriers **15-7**
Network Configurations **15-8**
Management of Networks **15-9**
Commercial Network Services **15-11**
Miscellaneous Communications **15-12**
Policies and Procedures **15-13**
Network Security **15-13**
Disaster Recovery **15-14**
Legally Enforceable Standards **15-14**
Risks and Controls **15-15**
Client/Server (C/S) Introduction **15-15**
C/S Background **15-15**
Role of Senior Management **15-16**
Definitions **15-17**
C/S Components and Characteristics **15-17**
Issues and Recommendations **15-18**

Chapter 15WP **Networking – Client/Server Workprogram** **15-21**
(FFIEC Disk #3 and File Name IS-WP#10.wpd)

Chapter 16 **End-User Computing** **16-1**
(FFIEC Disk #2 and File Name S2C16.wpd)
Concerns **16-2**
Standards **16-2**
Hardware and Software Selection **16-3**
Operations **16-4**
Disaster Recovery/Contingency Planning **16-4**
Networks and Telecommunications **16-4**
Small Systems **16-5**
Risk and Control Considerations **16-8**
Security **16-8**
Computer Operations **16-8**
Implementation and Maintenance **16-9**
System Software **16-9**
Database Management Software **16-9**
Middleware **16-9**
Conclusions **16-10**

Chapter 16WP **End-User Computing Workprogram** **16-11**
(FFIEC Disk #3 and File Name IS-WP#11.wpd)

Chapter 17 **Document Imaging** **17-1**
(FFIEC Disk #2 and File Name S2C17.wpd)
Definition **17-1**
Background **17-1**
Control and Security Risk Areas **17-2**
Components of the System **17-3**

Benefits 17-3
Risks 17-4
Implementation 17-4

Chapter 17WP Document Imaging Workprogram 17-5
(FFIEC Disk #3 and File Name IS-WP#12.wpd)

Chapter 18 Wholesale EFT (Electronic Funds Transfer) 18-1
(FFIEC Disk #2 and File Name S2C18.wpd)
Wholesale or Large-dollar Funds Transfer Systems 18-1
Controlling Payment Transfer Risks 18-4
Examination Concerns 18-5
Money Laundering and Wire Transfer Issues 18-10
BSA Recordkeeping for Funds Transfer Activities 18-10
Wire Transfer Control Considerations 18-11
Wire Transfer Message 18-11
International Enforcement 18-13
The Office of Foreign Asset Controls (OFAC) 18-14

Chapter 18WP Wholesale EFT Workprogram 18-17
(FFIEC Disk #3 and File Name IS-WP#13.wpd)

Chapter 19 Fedline EFT 19-1
(FFIEC Disk #2 and File Name S2C19.wpd)
Local Security Administrator 19-1
Miscellaneous Security Settings 19-1
User/Access Report Evaluation 19-2
Verification Fields 19-3
Verification Threshold 19-3
General Controls 19-3
Disaster/Contingency 19-4
Fedwire Wire Transfer Functions 19-4

Chapter 19WP FedLine EFT Workprogram 19-5
(FFIEC Disk #3 and File Name IS-WP#14.wpd)

Chapter 20 Retail EFT (ATM and POS) 20-1
(FFIEC Disk #2 and File Name S2C20.wpd)
Automated Teller Machines (ATM) 20-1
Point-of-Sale Systems (POS) 20-1
Debit and Smart Cards 20-3
Home Banking 20-3
Internal Controls for Retail EFT 20-4
PIN Control Guidelines 20-4
Plastic Card Control Guidelines 20-5
Terminal Sharing/Network Switching 20-6

Chapter 20WP Retail EFT (ATM and POS) Workprogram 20-7
(FFIEC Disk #3 and File Name IS-WP#15.wpd)

Chapter 21 Automated Clearing House (ACH) 21-1
(FFIEC Disk #2 and File Name S2C21.wpd)
Growth 21-1
Operators 21-1
Risks and Examination Concerns 21-1

Chapter 21WP Automated Clearing House (ACH) Workprogram 21-3
(FFIEC Disk #3 and File Name IS-WP#16.wpd)

Chapter 22 IS Servicing – Provider and Receiver 22-1
(FFIEC Disk #2 and File Name S2C22.wpd)
User Institution Controls **22-1**
Technology Controls **22-3**
Insurance for User Institutions and Servicer Providers **22-6**
Record Protection and Retention for User Institutions **22-7**
Contracts **22-8**
Contract Inducement Concerns **22-12**
Financial Information for User Institutions and Servicers **22-13**
Considerations for Service Receivers **22-14**
Potential Service Provider Issues **22-14**
Potential Service Receiver Issues **22-15**

Chapter 22WP IS Servicing – Provider Workprogram 22-17
(FFIEC Disk #3 and File Name IS-WP#17.wpd)

Chapter 22WP IS Servicing – Receiver Workprogram 22-23
(FFIEC Disk #3 and File Name IS-WP#18.wpd)

Chapter 23 Community Financial Institution IS Examination Program 23-1
(FFIEC Disk #2 and File Name S2C23.wpd)
Community Workprogram **23-1**
Introduction **23-1**
Rationale for Acquisition **23-1**
Evaluation of System Requirements **23-2**
Feasibility Studies **23-2**
Hardware and Software Concerns **23-2**
Data Conversions **23-5**
Contracting for Services **23-5**
Disaster/Contingency Planning **23-5**
Continuing Issues and Concerns **23-6**
Examination Process **23-8**

Chapter 23WP Community Financial Institution IS Examination Workprogram 23-11
(FFIEC Disk #3 and File Name IS-WP#19.wpd)

INTRODUCTION CHAPTER 1

(FILE NAME ON DISK # 1 = S1C1.WPD)

The 1996 Federal Financial Institutions Examination Council (FFIEC) Information Systems (IS) Examination Handbook (Handbook) is an interagency guide to assist regulatory examiners in examining information systems operations in financial institutions and independent service bureaus. It contains an overview of information systems concepts, practices, examples of sound IS controls, and FFIEC examination workprograms. It also covers regulatory policies of FFIEC member agencies for use in the examination of information systems. The FFIEC members are the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

In prior versions of this Handbook, its primary audience has always been identified as the experienced interagency IS examiner. Today, the audience includes: safety and soundness and other specialist examiners within each member agency; new or less experienced IS examiners; and the management of the financial institutions and service bureaus. The Handbook has also been expanded to serve as a:

- Tool for better supervision and examination guidance.
- Training aid for new IS examiners.
- Reference source for the industry under supervision.
- More comprehensive technical reference source.

Most Handbook sections have been reorganized and revised to reflect more accurately the rapidly changing information systems environment. Significant changes include:

- Development of several new narrative chapters and related work programs.
- Additional guidance on IS supervision by risk.
- Inclusion of a General and Administrative section.
- Significant modification of the Handbook's structure and presentation.

The numerous changes and modifications do not represent policy changes for the FFIEC or its member agencies. The Handbook has been updated to address emerging technologies in the financial and technology communities as they relate to IS safety and soundness issues and concerns.

The rapid growth of information systems technologies has caused significant changes in the way that financial institutions process data and information. Microcomputers (PCs) are shifting computing power from the traditional data center or service bureau to user departments. Telecommunications networks are enabling the distribution of IS resources throughout multi-site organizations. As a result, an institution's IS environment may include service bureaus, facilities management sites, in-house data centers, and end-user computers working together to meet its information processing needs. IS controls in each of these areas must be reviewed to ensure the accuracy and reliability of the institution's records and information resources. Examiners are also challenged to keep abreast of emerging and changing IS technologies to understand their risks.

Financial institutions must establish effective internal controls and develop management information systems to safeguard information and measure operating performance and profitability. Regulatory examinations evaluate the internal control systems affecting the integrity, reliability, and accuracy of data, and the quality of the management information systems supporting management decisions.

The examination strives first to identify risks that threaten the safe and sound operations of insured financial institutions. They can include:

- A catastrophic disaster.
- Inadequate management information reporting systems.
- Poor contracts with service bureaus or third party processing vendors.
- IS conversion failures.
- Significant applications processed on microcomputers or networks with inadequate controls.
- Security breaches.
- Mergers and acquisitions without proper review of IS resources.
- Legal or regulatory violations.

Risk analyses may also determine that special examinations of software vendors and IS conversions or technology projects are warranted. IS examiners may assist other safety and soundness or compliance examiners in reviewing IS risk areas during non-IS examinations.

Chapter 2 describes the IS Supervision by Risk approach. This approach is an evolving policy area emphasized increasingly by all financial regulatory agencies. The chapter serves as guidance only and is supplemented and supported by FFIEC member agency specific policy issuances. This approach is intended to ensure that agency supervisory resources are applied appropriately to supervisory areas of concern based on the degree or level of risk.

This Handbook is being printed as two volumes. A companion package of four disks supporting the Handbook is being mailed separately to holders of the Handbook.

- **Volume 1** includes **Sections I and II** and covers the purpose of IS examinations; the IS control structure; and guidance to IS examiners and the workprogram steps for an IS examination or review.
- **Volume 2** includes **Sections III and IV** and covers the reference material that support the IS supervisory process.

Occasionally a reference appears in the Handbook to a particular manufacturer or corporation. They are not endorsements of those organizations or products.

This Handbook and the accompanying disks will continue to be updated biannually to reflect changing information systems technologies and regulatory agency guidance.

Several FFIEC member agencies have also established Internet home pages which may be referenced going forward to access evolving agency IS policies. Member agency Internet home page addresses are noted following the title page (page iii) of this Handbook.

IS SUPERVISION BY RISK

CHAPTER 2

(FILE NAME ON DISK # 1 = S1C2.WPD)

FFIEC member agencies supervise all financial institutions according to a philosophy based on providing high quality supervision. This supervision is directed at identifying existing or potential problems, and ensuring that problems are corrected. Because banking is essentially a business of accepting and managing risk, that philosophy is centered on evaluating risks. FFIEC member agencies apply that philosophy in all supervisory activities they conduct, including IS examinations.

Regulators must communicate with individual institutions and the industry to influence the change necessary to assess, monitor, and control risks appropriately.

Institution management is responsible for controlling risk. Regulatory agencies assess the quality of risk management, conducting oversight rather than audit. This type of supervision concentrates on systemic issues and institutions or areas that pose the greatest risk to the system.

FFIEC IS RISK OVERVIEW PROGRAM

Each FFIEC member agency maintains an IS regulatory program responsible for identification and reduction of unwarranted risks that could threaten a healthy system of financial institutions. The programs are supported by a small cadre of specially trained IS examiners who examine information systems and technology posing the greatest levels of transaction risk. IS examinations of institutions and independent vendors are designed to supplement other types of examinations (safety and soundness, compliance, fiduciary, etc.) of federally insured financial institutions. The timing and scheduling of IS examinations are determined by a number of factors including risk analysis results, inter-agency coordination at district and national levels, and intra-agency coordination with other types of examinations.

The IS regulatory program is based on the concept of Supervision by Risk. IS regulatory staff is directed by each agency's management to entities with high risk conditions or profiles (e.g. large, complex, or difficult to review information systems environment) affecting institutions under their jurisdiction. Supervision by Risk involves the selection of entities warranting examinations by IS examiners, followed by the development of a risk based supervisory strategy for each entity. This approach provides for analysis of examination coverage by IS examiners of all institutions and independent vendors in areas such as EFT switches, service bureaus, bill payment processors, software vendors, disaster recovery services, etc. Institutions, their independent vendors, and emerging risk areas are monitored and evaluated regularly by each agency's management for inclusion in the caseload for IS examiners.

RISK DEFINITION

Risk is the potential that events, either expected or unanticipated, may have an adverse impact on the institutions' or firms' earnings or capital. The existence of risk is not a reason for concern. Rather, examiners must determine if the risks are warranted. Generally, risks are warranted when they are: understandable, controllable, and within the institution's capacity to readily withstand adverse performance. When unwarranted risk occurs, whether deliberate or unintentional, examiners must communicate with management to mitigate risks by controlling or limiting exposure. Appropriate actions would normally include reducing exposures, strengthening controls, increasing capital, and ensuring the presence of an effective level of policies and procedures.

IS examiners primarily focus on transaction risk. These risks are associated with service or product delivery, and with providing support in all management processes (e.g., information for decision making and financial control). Transaction risk is present in all products, services, and aspects of an institution's operations (including at vendor locations). A major thrust of the IS examination is reviewing the effectiveness of management information systems and technology.

RISK ANALYSIS

An IS risk analysis assists examiners in developing a risk based supervisory strategy. This includes setting examination scope and objectives and identifying appropriate examination procedures necessary to support the overall strategy.

Time spent on examining areas should be commensurate with the level of risk that is present. Examiners will perform a risk analysis at least once during each supervisory cycle. An optional risk analysis form is located in the following workprogram. It describes one method that can be used in measuring and assessing risk.

Measuring and Assessing Risk

A common framework to document decisions about risk ensures effective supervision and consistency. Risk analysis is intended to provide examiners with a concise method of communicating and documenting judgments about the quantity of risk and quality of risk management and aggregate levels of risk. Risk assessments give both a current and prospective view of the institution's or independent vendor's risk profile.

The following approach for measuring and assessing risk is presented as an example and represents one such methodology. Each FFIEC member agency has the latitude to adopt policies or approaches representing different methods of risk analysis.

IS examiners must make judgments on the following as they affect transaction risk:

- *Quantity of Risk* – This refers to the level or volume of risk present. The assessment notes if the level of risk is high, moderate, or low.

- *Quality of Risk Management* – This refers to how well risks are identified, understood, and controlled. Assessments are weak, acceptable, or strong.

- *Aggregate Risk* – The assessment is a summary judgment incorporating both the quantity of risk and the quality of risk management. It allows the examiner to weigh the relative importance of each factor for a given institution and directs specific activities and resources for supervisory strategies. This is categorized as high, moderate, or low.

- *Direction* – This reflects the examiner's views on likely changes to the risk profile over the next supervisory cycle. Direction is expressed as decreasing, stable, or increasing. Decreasing indicates that the examiner anticipates, based on current information, the aggregate risk will decline over the next 12 months. Stable indicates the examiner anticipates the aggregate risk profile will remain unchanged. Decisions on the direction of risk may influence the supervisory strategy.

The institution's risk profile should guide the supervisory strategy and examiner resources employed.

Quantity of Risk

When assessing the quantity of risk, the IS examiner should consider:

- Transaction dollar exposure relative to earnings and capital of financial institutions.

- Transaction volume relative to the information system's capacity.

- Changes in ownership or management.

- The complexity of hardware and software systems and stability (current and projected) of these systems.

- The volume and risk exposure relative to the internal control exceptions.

- The potential for significant financial loss due to:
  - Human error or fraud.
  - Competitive disadvantage.
  - Incomplete information.
  - Operational disruption.

- The history of litigation relative to operations.

- The adequacy of controls over outsourcing arrangements.

- The examiner should also consider new activities that are not readily quantified (e.g., current emerging concepts with Internet activities.)

A review of those factors should allow the examiner to quantify the aggregate transaction risk to one of the following risk categories:

- **High** – The level of transaction processing and state of systems expose the institution or system of financial institutions to significant damage to reputation or loss of earnings or capital. The institution may have a history of transaction processing failures. The likelihood of future processing failures remains large because of the absence of effective internal controls.

- **Moderate** – The state of systems adequately supports the level of transaction processing. The volume and complexity of activities expose the institution to a degree of risk. Possible losses to reputation, earnings, or capital exist, but are mitigated by adequate internal controls.

- **Low** – The level and complexity of transaction processing is low and well supported by the state of systems development. Possible damage to reputation; loss of earnings; or capital is slight. The institution has a history of sound operations. The likelihood of future transaction processing failures is minimal in the presence of strong internal controls.

Quality of Risk Management

Risk analysis involves an assessment of the quality of risk management. Institutions successful in risk taking are those that have a corporate culture that balances controls and business initiatives. No single system works for all institutions, because conditions and organizational structures vary. Each institution should have its own risk management program tailored to its individual needs and circumstances. Sound risk management systems have several common fundamentals. For example, all risk management systems should be independent of risk-taking activities. Regardless of the risk management program's design, each should include:

- Risk Identification – Proper risk identification strives to recognize and understand existing risks or risks that may arise from new business initiatives. This should be a continuing process.

- Risk Measurement – Accurate and timely measurement of risks is critical to effective risk management systems. The lack of a risk measurement system inhibits the ability to limit or monitor risk levels. The sophistication of measurement tools should be suited to the complexity and levels of risk assumed. Periodic tests should be performed to validate the integrity of the measurement tools.

- Risk Control – Limits should be established and communicated through policies, standards, or procedures that define responsibility and authority. These control limits should be meaningful management tools that may be adjusted to changes in conditions or risk tolerances. A process should exist to authorize and monitor exceptions to risk limits when warranted.

- Risk Monitoring – Risk levels should be monitored to ensure timely review of risk positions and exceptions. Reports should be frequent, timely, accurate, and informative and should be distributed to appropriate persons to ensure action.

Effective risk management is more than merely a process comprised of those controls. It requires an informed board, capable management, and appropriate staffing. The board must guide the institution's strategic direction by approving policies that endorse the organization's risk tolerance. Well designed monitoring systems allow the board to hold management accountable for operating within established tolerance levels.

Capable management and appropriate staffing are critical to effective risk management. Institution management is responsible for the implementation, integrity, and maintenance of risk management systems. Management must also keep the directorate adequately informed. In discharging its role, management:

- Implements the company's strategic direction.

- Defines the institution's risk tolerance through the development of policies that are compatible with strategic goals.

- Develops management information systems that are timely, accurate, and informative.

- Ensures that strategic direction and risk tolerance are communicated effectively throughout the organization.

Examiners assess risk management systems by considering policies, processes, personnel, management, and control systems. A significant deficiency in one or more constitutes a deficiency in risk management. Uncorrected, the deficiency could affect adversely the institution's earnings, capital, or standing in the community by reflecting poorly on its intent, commitment, and ability to perform.

Examiners assess the quality of risk management by considering:

Whether policies are:

- Comprehensive, including whether they:

– Establish responsibilities and accountability.
– Set standards for systems development, changes,

– Provide for contingency planning.

- Consistent with strategic direction and risk tolerance levels.
- Approved by the board or an appropriately delegated committee, as necessary.

Whether a process exists for:

- Communicating related policies and expectations to appropriate personnel.

- Approving and monitoring compliance with policy limits.

- Responding to changing market conditions.

- Identifying information needs to manage the corporation efficiently.

- Defining the systems architecture for transaction processing and for delivering products and services.

- Developing and maintaining systems for product and service delivery.

- Monitoring system capacity and performance.

- Assuring the integrity and security of systems and the independence of operating staff.

- Documenting system (programming) history adequately.

- Assuring the reliability and retention of information (e.g., data creation, processing, storage, and delivery). This includes business continuity planning.

- Establishing effective internal administrative and accounting controls.

- Undertaking due diligence assessments.

- Ensuring the adequacy of controls over outsourcing arrangements.
- Providing the timely production and use of management information.

Whether personnel:

- Understand strategic direction, risk tolerance limits, and policies.
- Exhibit technical and/or managerial competency in relation to the complexity of products.

- Are sufficient in number and skills for current and anticipated needs.

- Are adequately compensated so that turnover is limited and stability fostered.

Whether management:

Demonstrate a commitment to training, development, and continuing education programs.

- Demonstrate a commitment to providing an effective performance management program.

- Ensure independence, expertise, and competency in performing control functions, such as loan review or audit.

Whether control systems are designed to provide:

- Timely, accurate, and meaningful management information.

- Independent and effective feedback on compliance with policies and operating procedures. Control systems should be consistent with the complexity of the activities, but, at a minimum, should include internal and/or external audit reviews.

A review of those factors should allow examiners to assess and rate the quality of transaction risk management in an institution. The rating, described as weak, acceptable, or strong according to the following guidelines, should be incorporated as appropriate into the overall rating for management.

- **Weak** – Responsible officials do not understand, or have chosen to ignore, key aspects of transaction risk. Management does not anticipate or take prompt or appropriate actions in response to changes in the market or technology. Policies to control transaction risk do not exist or are inadequate. Serious weaknesses exist in operating and information systems, internal controls, internal and external audit coverage, or contingency plans. Management information on transaction processing activities exhibits significant weaknesses. Planning or due diligence may be inadequate, allowing exposure to risk by introducing new products and services or acquisitions. There may be exposure to processing risks due to poor conversion management, either from integration of new acquisitions with existing systems, or from converting one system to another. Management has not demonstrated a commitment to make the corrections required to improve transaction processing risk controls.

- **Acceptable** – Responsible officials reasonably understand the key aspects of transaction processing risk. Management responds adequately to changes in the market or technology. Management identifies and measures the most significant processing risks. Policies exist that address exposure to significant processing risks. Procedures may contain only modest deficiencies. Adequate operating and information processing systems, internal controls, audit coverage, and contingency plans are evident. Minor deficiencies may exist in management information that relates to transaction and information processing activities.

- **Strong** – Responsible officials fully understand all aspects of transaction processing risk. Management anticipates and responds well to changes of a business, economic, market or technological nature that affect processing risk. Management has comprehensive policies addressing transaction processing risks. Implementation plans are clear and followed. Systems, internal controls, audit and contingency plans are sound. Management has demonstrated favorable performance in acquisitions and the introduction of new products and services. Management identifies weaknesses quickly and takes appropriate action.

SUPERVISORY STRATEGIES

A supervisory strategy is a plan to provide effective, efficient supervision for each organization. Those dynamic documents are reviewed and updated regularly based on the organization, industry, and economic developments. The following optional workprogram may help provide guidance for the development of a supervisory strategy. Each FFIEC member agency is responsible for the development of its own policies on developing risk based supervisory strategies.

The IS EIC prepares the strategy which is reviewed subsequently by the next higher level of management. The supervisory strategy directs examination activities and is based on:

- Statutory and policy based examination requirements.

- Agency standards and priorities.

- Knowledge of the institution including:

  - Risk profile.
  - Strengths and weaknesses.
  - Supervisory history.
  - Market factors.

Elements of a Supervisory Strategy

The three primary elements of the supervisory strategy are:

Objectives – Document the EIC's goals for supervision of the institution based on its risk profile and appropriate statutory or agency standards. They are the foundation for all activities and work plans. Well defined objectives provide for focused and efficient examination activities and help managers ensure consistent and appropriate application of supervisory policy. Supervisory objectives must be clear, attainable, specific, and action-oriented.

Activities – Detail steps that will achieve supervisory objectives. Each activity should link directly to one or more of the supervisory objectives. They should be focused on ensuring that risk management systems operate effectively. Activities should include a plan for communication with the institution, detailing the types and frequency (e.g., report of examination, meeting with the board of directors, etc.)

Work plans – Include methods for achieving strategies. They provide details that outline the scope, timing, and resources needed to meet supervisory objectives and strategies.

Risk Analysis

Examiners should complete a risk analysis at least once during each supervisory cycle.

Name of Institution City/State

Examiner-in-Charge Date

Reviewed by Date

1. The quantity of transaction risk is :

_____high____moderate____low

2. The quality of transaction risk management is:

____weak____acceptable____strong

3. Aggregate transaction risk is:

____high____moderate____low

4. The direction of change in transaction risk is expected to be:

____increasing____stable____decreasing

Provide narrative support to the assessment. Use additional pages as necessary.

Note: This workprogram form is a sample tool and its use is determined by policy within each FFIEC member agency.

Supervisory Strategy

Supervisory strategies are dynamic documents. Examiners should review and update strategies regularly based on the organization, industry, and economic developments.

Name of Institution	City/State
Examiner-in-Charge	Date
Reviewed by	Date

Based on the institution's risk profile and appropriate statutory and agency standards, prepare a supervisory strategy addressing the following, using additional pages as necessary:

Objectives – Define the goals of supervision for the institution. The goals should be clear, attainable, specific, and action-oriented.

Activities – Identify the steps that will achieve the supervisory objectives. Each activity should link directly to one or more supervisory objective. Activities should include a plan for communications with the institution detailing the types and frequency of communications (e.g., report of examination, meeting with the board of directors, phone calls, E-mail, etc.)

Work Plans – Describe how strategies will be achieved. Include details on the scope, timing, and resources needed to meet supervisory objectives and strategies.

Note: This workprogram form is a sample tool and its use is determined by policy within each FFIEC member agency.

Aggregate Risk Matrix

Quality of Risk Management	Low	Moderate	High
Weak	Moderate	High Moderate Quantity Precludes "Highest"	Highest
Acceptable	Low Acceptable Risk Management Precludes "Lowest"	Moderate	High Acceptable Risk Management Precludes "Highest"
Strong	Lowest	Low Moderate Quantity Precludes "Lowest"	Moderate

Quantity of Risk

Note: This matrix is only a graphic representation of a risk decision process; it is not a required interpretation. The matrix represents the aggregate risk assessment based on the quantity of risk and the quality of risk management for each type of risk. The aggregate risk decision may be affected further by mitigating factors. Examiners can use a similar, one-dimensional risk matrix for composite risk decisions.

EXAMINATION PLANNING CHAPTER 3

(FILE NAME ON DISK # 1 = S1C3.WPD)

The IS regulatory program supports the overall goal of financial institution and servicer regulatory reviews. The reviews are designated to identify and correct information on technology-related risk exposures of significance that threaten the financial institutions industry. The information is updated regularly to encourage uniformity among FFIEC member agencies in regulating financial institutions and their service bureau vendors. A properly directed and managed IS regulatory program may be achieved by:

- Supervising IS program performance, including program development, quality control, and staff development.
- Maintaining a risk-based IS program for allocation of limited IS examination resources.
- Scheduling IS examinations.
- Supervising work to ensure alignment with safety and soundness objectives.
- Supervising work completeness, accuracy, and conformance with regulatory policies and procedures.
- Distributing IS reports of examination of institutions and service bureaus.
- Reviewing written response to report findings.

IS EXAMINATION TYPES

IS examiners are responsible for examining service bureaus, in-house data centers, and other high risk situations (e.g., systems conversions in serviced institutions). The types of IS examination activities performed by FFIEC IS examination departments are as follows.

Institution Operations

- *In-house* – Institution that operates its own data center and does not service others (if other institutions are serviced, the institution should be treated as a local or regional service bureau).
- *Serviced* – Institutions serviced primarily by service bureaus.
- *Interagency Shared Application Software Reviews (SASR)* – Interagency reviews of widely used turnkey software products. SASR reports are distributed by agencies for internal use only.

Service Bureau Operations

- *MDPS* – Multiregional data processing servicers that may be regional or national in scope and that service more than one class of financial institutions.
- *National* – Service bureaus that are not part of the MDPS program and that service financial institutions on a national scale.
- *Regional* – Service bureaus that service financial institutions on a less than national scale but that have locations in a sufficient number of contiguous states to be considered regional in scope.
- *Local* – Service bureaus that service one or more institutions in the same region.

FREQUENCY OF IS EXAMINATIONS

The frequency of in-house and service bureau examinations is based on the concept of risk based supervision/regulation, i.e., the lower the risk, the less the regulatory scrutiny. FFIEC member agencies direct resources to those data centers or situations that need greater supervisory attention. The lower the rating, (4 or 5), the more closely the data center is monitored and more frequently examined. Data centers assigned higher and better ratings, (1 or 2), generally require less regulatory scrutiny. Other factors that might prompt more frequent examinations include a deteriorating condition, enforcement action, substantial plans for IS replacement, or a change of control. The frequency of

in-house institution examinations is determined by the policy of each FFIEC member agency.

Service Bureaus

Service bureau examinations which generally are not linked to a safety and soundness examination of a financial institution are scheduled under separate criteria. In all cases the IS examinations of regional and local service bureaus must be coordinated with other regulatory agencies. Service bureaus in the national Multiregional Data Processing Servicer (MDPS) Program are examined on an interagency basis and administered and coordinated through the Washington office of each agency.

The examination schedule for service bureaus should consider the risk level of serviced institutions as discussed under the supervision by risk concept (see Chapter 2 for additional information.)

Serviced Institutions

IS-related risks in institutions' serviced primarily by service bureaus are examined by safety and soundness examiners using appropriate procedures. These examinations are normally part of the regularly scheduled safety and soundness examination.

Shared Application Software Reviews

Interagency Shared Application Software Reviews (SASR) of vendor turnkey software products will be performed periodically (generally one per quarter) as determined by the FFIEC IS Subcommittee. SASR reviews document the characteristics of the software products to assist examiners in examining institutions using the vendor products. There are no ratings for these reviews. Districts/regions, at their discretion, may perform software reviews on selected turnkey software products that are used widely by institutions in their region.

TIME STANDARDS FOR IS EXAMINATIONS

The intent is for IS examinations of in-house institution data centers to be conducted concurrently with those for the safety and soundness supervisory efforts in a financial institution. IS examinations of service bureaus should be performed for both MDPS and non-MDPS jointly with other supervisory agencies. Each agency has developed procedures and guidelines for scheduling and conducting IS examinations to allocate IS examination specialists properly. These scheduling procedures should be adjusted and the institution notified when the IS examination cannot be performed concurrently with the safety and soundness examination,.

Time allocated for an on-site IS examination is based on the risk and complexity of the examination. After arrival on-site the IS EIC should validate the scope and risk assumptions to ensure time planned is adequate to address the identified risks. If additional on-site examination resources are required the IS EIC, must consult with the safety and soundness EIC on concurrent examinations and/or with the IS examination manager to evaluate the request for more resources. If approved, the IS EIC must reevaluate and modify the examination scope to schedule the use of any additional resources.

Shared Application Software Review (SASR)

One examiner from each agency is normally assigned for two weeks to each SASR review. The lead agency's EIC may work for up to three additional weeks to finalize the SASR report. The additional time commitment depends on the complexity of the product, scope of prior planning, and extent of vendor support received.

FINANCIAL INSTITUTION EXAMINATIONS

IS examinations of in-house institution data centers should be conducted concurrently with safety and soundness examinations according to member agency policy. Safety and soundness and IS examiners should work together as a team. The safety and soundness EIC may include statements on the IS examination findings in the safety and soundness report.

Each agency's organizational structure, position titles, and responsibilities vary. Guidelines for conducting concurrent IS examinations are developed by each agency. The procedures should be adjusted accordingly when the IS examination cannot be performed at the same time as the safety and soundness examination.

The relationship between the safety and soundness EIC and the IS EIC is similar for all agencies. Although

agency organizational structures, IS related job descriptions, and reporting lines differ, they ascribe essentially the same duties to the IS examiner.

IS Examiner-in-Charge Responsibilities

The IS EIC is responsible for the administration and overall performance of the IS examination. These responsibilities include, but are not limited, to:

- Performing sufficient planning to identify and evaluate IS risk areas and ensuring that the scope of IS examination covers high risk activities. Reviewing internal and external audits to supplement the examination process.

- Preparing IS examination objectives and procedures for activities included in the scope.

- Preparing a project plan containing scope, objectives, procedures and often a budget; the examiner allocation should reflect a breakdown of total hours and a schedule for significant scope activities.

- Prior to the start and during concurrent examinations, discussing and resolving scoping and resource and administrative issues with the safety and soundness EIC.

- Keeping the safety and soundness EIC and IS examination manager informed of scheduled meetings with management and attending meetings.

- Ensuring that the examination procedures are completed in accordance with the appropriate sections of the *1996 FFIEC IS Examination Handbook* and with the approved project plan.

- Communicating examination findings to the IS examination manager and safety and soundness EIC.

- Holding exit meetings with IS management to review findings of the examination and recommendations for follow-up.

- Preparing a "camera ready" ROE with an assigned rating and clear, concise summary of findings. The ROE should reference the objectives of the scoping document and workprogram and be supported by workpapers.

- Signing IS ROE. The ROE must be signed by an accredited IS examiner.

- Forwarding the IS ROE to the IS examination manager for review; incorporating review comments as appropriate, and forwarding "camera ready" IS ROE to the safety and soundness EIC.

- Conducts the IS portion of safety and soundness board of directors meetings for 4- and 5-rated institutions. The IS examination manager should participate in these meetings as appropriate.

- Reviewing and evaluating IS examiners.

Supporting IS Examiner Responsibilities

- Performing assigned workprogram sections per FFIEC examination guidelines.

- Documenting findings in workpapers and finding sheets.

- Identifying deficiencies and communicating significant findings to the EIC and other examiners.

- Discussing findings with management.

- Ensuring that workpapers are cross-referenced properly to document, and support substantial findings and conclusions.

- Preparing findings and recommendations in "camera ready" report format.

Safety and soundness Examiner-in-Charge – responsibilities of the safety and soundness EIC include:

- Working closely with the IS EIC on planning and performance of concurrent examinations, scheduling of management meetings, and resolving related IS examination issues.

- Attending opening and closing meetings and other meetings at which significant IS issues are discussed, when concurrent examinations are conducted.

- Reviewing IS ROE and considering IS examination findings to determine the adequacy of the institution's system of internal controls and safety and soundness ratings.

- Incorporating significant IS findings in the safety and soundness ROE, as appropriate, and attaching the OPEN section of the IS ROE as an addendum to the safety and soundness ROE.

- Conducting board of directors meetings.

- Modifying regulatory plan, as necessary.

IS Examination Manager – The IS examination manager's responsibilities include:

- Ensuring that district/regional IS examining resources are used effectively based on risk profile of supervised institutions.

- Coordinating requests for financial institution, service bureaus, and MDPS IS examinations from agency management. Monitoring revisions to IS examination schedule and adjusting as necessary.

- Assigning an IS EIC and supporting examiners.

- Reviewing and signing or recommending for signature the final IS ROE for the district/region.

- Supervising the performance of IS examinations and high risk situations (e.g., system conversions). Coordinating MDPS examination activities with Washington headquarters and the MDPS EIC.

- Ensuring the overall quality, competency and consistency of IS examinations, and compliance with national and FFIEC standards.

- Conducting meetings with management and boards of directors.

- Reviewing service bureau ROE's and collaborating with agency/interagency management for distribution to the service bureaus, IS client serviced institutions, and to other regulatory agencies.

- Reviewing management responses to findings in ROE.

SERVICE PROVIDERS' EXAMINATIONS

Agency management must ensure that all service bureaus within its area of responsibility receive IS examinations as required member agency and FFIEC policy. Most, if not all, of the activities and responsibilities of the IS EIC, supporting IS examiners and to a lesser extent the IS manager are the same in a service provider examination.

IS Examiner-in-Charge Responsibilities

In a servicer examination the IS EIC is responsible for:

- Communicating examination findings to the IS examination manager and EIC for interregional or interagency service bureau examinations.

- Holding exit meetings with service bureau management to review examination findings and recommendations for follow-up.

- Forwarding ROE to IS examination manager for review. Incorporating review comments and providing final copy to IS examination manager.

- Conducting IS board of directors meeting for service bureaus.

- Reviewing and evaluating IS examiners.

- Assisting in scheduling interagency examinations.

- Reviewing scope documents for MDPS examinations.

IS Examination Manager – The IS examination manager's responsibilities include:

- Preparing the transmittal letter for the servicer's board of directors.

- Reviewing MDPS ROE's.

- Sending MDPS ROE's to service bureaus and districts/regions.

MDPS Examiner-in-Charge

In addition to the duties previously described in the Examiner-in-Charge Responsibilities section the MDPS

EIC will be responsible for:

- Scheduling and setting the scopes of MDPS examination of corporate headquarters and remote data centers, based on input from all effected agencies.

- Coordinating resources to conduct examinations under guidance from Washington headquarters.

- Reviewing individual MDPS data center ROE's and resolving examination issues with other agency personnel.

- Preparing MDPS ROE, assigning rating and signing the ROE.

- Sending ROE to Washington headquarters for final review. Distribution occurs from the agency headquarter's office or the district or region, as appropriate.

- Reviewing service bureau responses to ROE findings and distributing to Washington headquarters.

GATHERING INFORMATION

The IS EIC must gather, organize, and analyze available information prior to beginning an on-site IS examination. Sources of information include, but are not limited, to:

- The IS examination permanent file.

- The supervisory/regulatory plan for the financial institution.

- Prior examination reports, workpapers, and recommendations.

- Supervisory actions and correspondence.

- Internal and external audit reports, when available.

- External databases (NEXIS/LEXIS). Discussions with appropriate regional personnel and other agencies.

SCOPING THE EXAMINATION

Effective examinations must be properly pre planned to ensure that significant IS risks are identified and appropriate regulatory action taken. Once the risk areas have been identified the examination planning scope involves reviewing available information to determine specific examination procedures to be performed and the depth of coverage (e.g., Tier I and Tier II).

The IS EIC must determine the scope of work and estimate the hours required to complete it. The examination of all potential risks should consider staffing, time, and benefits. Adequate time must be allocated to higher risk activities. In service bureau examinations that assess more than one data center, the scope document should include the headquarters location and all subsidiary data centers.

Scoping procedures should emphasize risk areas. Some of the risk areas that should be considered while developing the scope are: IS audit adequacy, management planning/direction, conversion activity(s), application development/maintenance, data/system/physical security, networking, corporate contingency planning activities, and computer system controls.

After the scope of examination is determined, an IS examination scope memorandum is prepared to document the areas to be examined. The scope memorandum should outline the objectives of the examination, assignments, budget, and other relevant information. When examining in-house data centers, the examiner should visit the data center and talk to the IS management. He/she should gather basic information to aid in: identifying high risk areas and known problems, and determining the size and complexity of the data center and software systems. On concurrent examinations, all meetings with IS management should be coordinated with the safety and soundness EIC. On MDPS examinations, all meetings with the servicer senior management should be coordinated with the lead agency MDPS EIC and Washington headquarters.

The initial examination scope is based on preexamination analysis and on-site review of IS data processing and management information systems. It should be refined at the start of, and during, the examination as additional information is obtained and reviewed. Off-site materials that should be considered in determining the scope are listed in the previous section on Gathering Information. The preliminary

scope provides information to determine staff requirements, the examination start date, and strategies for conducting the examination. Upon starting the on-site activity, additional information that may affect the scope should be reviewed as soon as possible.

During the task of setting the scope and throughout an examination, the IS EIC should maintain regular communications with the safety and soundness EIC, IS examination manager, MDPS EIC, and other agencies, as necessary. Anticipated significant changes in scope, projected staffing, and completion dates should be communicated promptly to the appropriate persons. The team should know the regulatory plan objectives and the approach for meeting them. In that regard, the IS EIC must communicate effectively with the safety and soundness EIC and team members.

COORDINATING THE EXAMINATION

IS examinations of institutions with in-house data centers should be conducted concurrently with safety and soundness examinations. In planning and coordinating those IS examinations, the IS EIC works closely with the safety and soundness EIC. The safety and soundness EIC should be kept informed of the status of the IS examination. The examination activities on service bureau examinations, should be coordinated with the IS examination manager and other staff.

When conducting concurrent examinations, the safety and soundness EIC should be advised of the following information at the start of, and during the examination:

- The IS examination start date.
- The time and location of meetings with management.
- The IS examination scope and schedule.
- Interim status and progress reports as required by IS manager.
- Any material findings or modification of examination scope.
- The agenda for the exit conference prior to meeting with management.
- Drafts of the proposed IS ROE and the transmittal letter.

Sometimes, IS examinations of in-house centers may be conducted separately from safety and soundness examinations. The IS EIC should coordinate the IS examination work with the safety and soundness EIC.

Joint Examinations

The IS examiner may participate in joint IS examinations of service bureaus with other districts and federal or state agencies. Those examinations require that the scoping, scheduling, and preparation of the ROE be coordinated with the other agencies. For other joint examinations, IS examiners must be flexible and cooperative when working with other districts/regions and regulatory agencies.

NOTIFICATION OF THE EXAMINATION

For concurrent examinations, the institution will be notified in the safety and soundness request letter that an IS examination will be conducted. When conducting separate IS examinations, the notification letter should be mailed at least four weeks prior to the start of the examination. The letter should be addressed to the Chief Executive Officer (CEO) of the institution or servicer and signed by appropriate regulatory personnel. The letter should be sent to appropriate safety and soundness personnel and key contact people at the institution. For service bureau examinations, a client list may also be requested in the notification letter or in a separate request letter.

For service bureau examinations, the IS EIC or IS examination manager contacts the IS examination contact person prior to starting the examination. The initial communication should inform the service bureau management that an IS examination has been scheduled, the date, requested information, the name of the EIC, and other details.

At least one week prior to the projected start date, the IS EIC should call the institution or servicer to verify that the letter was received, to answer any questions, and to make arrangements for on-site work. The IS examiner will have frequent contact during the examination with the management of both the internal audit department and the data processing department. It is appropriate to meet initially with them and their staff. At the start of the examination this management meeting should be scheduled on-site to discuss:

- New developments since the last audit and/or examination, i.e., changes in control or management.
- Actions taken to correct deficiencies mentioned in prior examination and audit reports.
- Operating performance in comparison with the budget.
- Significant changes in operations or strategies.
- Significant concerns of management.
- Economic and competitive conditions in market area.
- Significant planned or anticipated changes and developments in IS hardware or software.

The introductory or later meetings may also address:

- Time limits for receiving requested information.
- The availability of the examiners to answer questions from the staff preparing requested information.
- Administrative details, such as names of key contact people, facilities and parking, work hours, and use of equipment.
- The duration of the examination, any planned interruptions (these should be kept to a minimum), names of examiners, and methods to ensure the efficient use of examiner's time.
- A meeting with the independent auditor, if applicable.
- Review of independent audit workpapers.
- Timing for regular meetings with the CEO to discuss the progress of the examination and to address any other issues of concern to the CEO or the IS EIC.

EXAMINATION PLANNING WORKPROGRAM

CHAPTER 3WP

(FILE NAME ON DISK #3 = IS-WP#02.WPD)

Comments

This section is intended to assist the examiner in planning the examination. It provides an overview of the nature and extent of information systems activities being performed by and for the institution. This document will included in the workpapers. The examiner must:

1. Coordinate with appropriate agency personnel any preliminary materials, procedures, or other documentation that should be reviewed or developed for the examination. Develop and mail examination request/first day letter and review any material received about the institution.

2. Review the following matters relevant to the current examination:

   - The previous report of examination and any other reports used to monitor the condition of the institution and its affiliates.

   - The correspondence file, including any memorandum relevant to the current examination.

   - Audit reports and third party reviews of outside servicers when available that provide significant IS support to the institution.

   - IS rating of the institution and independent industry rating and information servicers, which may include the IS CAMEL rating, as applicable.

3. During the pre-examination, discuss with appropriate institution and data center officers and obtain current information on:

   - Important developments since the last examination (including staffing, management, and internal audit operations).

   - Significant planned or probable developments. This may include relocations, mergers, acquisitions, major system conversions, changes in hardware and software, or major contract services.

   - Important changes in the institution's policies that

affect IS.

- Additions and/or deletions to customer services.

- General level of IS support the institution receives from outside servicers, if any.

4. Determine the source of such major IS support as:

   a. In-house data center.

   b. Facilities management.

   c. Vendor.

   d. External DP servicer.

   If b, c, or d is selected, provide the:

   - Vendors' names.
   - Applications supported.
   - Operating systems.
   - Types of hardware (e.g., micro, mini, mainframe).

5. Request information about the condition of a major servicer(s) who provides IS servicing to the institution.

6. If micro/mini systems are used to support significant applications, identify the type of hardware, purchased software, and the applications or functions supported.

7. Determine if the institution has significant networking/teleprocessing operations. Indicate the applications and functions supported.

8. If the institution's data center provides IS support to other financial institutions or business entities, obtain data on serviced customers. This may include:

   a. Institution name, type of institution, bank/association, or other identifying information.

   b. Name and address (city, state) of the institution.

CONCLUSIONS

10. From the materials reviewed, determine if significant changes have occurred in operations that might affect the timing, staffing, and extent of testing necessary in the examination.

11. Prepare the examination plan.

12. Assign assisting examiners to the applicable areas. Specify in the procedures of the applicable sections the level of testing anticipated.

13. Provide any additional information that will facilitate future examinations.

Examiner | Date
_____|_____

Reviewer's Initials

EXAMINATION TECHNIQUES CHAPTER 4

(FILE NAME ON DISK # 1 = S1C4.WPD)

ON-SITE PROCEDURES

The IS EIC must direct and control the on-site examination to ensure that its objectives and scope are met. Examiners must gather information to support the conclusions reached during the examination. All conclusions must be properly documented and maintained in the examination's working papers.

Examiners may obtain documentation by inspection observation, inquiry, confirmation, or analytical tests. Various forms of support may be collected, whether physical, testimonial, documentary, or analytical and maintained in the working papers. In obtaining and evaluating information, the examiner must select the strongest documentation for inclusion in the working papers.

To maintain an adequate level of control over the examination, the IS EIC must:

1. Meet with the senior IS officer or designee at the beginning of the examination.

2. Coordinate with examination staff the review of the IS request letter materials obtained from the institution or service bureau.

3. Make adjustments to examination scope as necessary.

4. Notify the IS examination manager and safety and soundness EIC, if appropriate, if significant changes are anticipated in scope, staffing needs, duration, etc.

5. Ensure that information requested from management is received and distributed promptly.

6. Throughout the examination:

   - Review continuously the work flow, findings, conclusions, and actual versus budgeted time, and take appropriate actions for the effective use of time.

   - Discuss all items of concern with assisting examiners, the IS examination manager, and the safety and soundness EIC, so that accurate information is presented at the closing conference.

   - Keep senior and IS management informed of significant issues during the examination.

   - Determine that all examination work is being prepared in accordance with policies, including workprograms, workpapers, conclusion memos or exception sheets, draft comments, report pages, and time sheets.

   - Review all examination work as it is being completed, including workprogram sections, conclusion memos, draft comments, and report pages.

   - Discuss the closing meeting agenda with management prior to the actual meeting.

7. Attend board of directors meetings as appropriate.

8. On separate institution and service bureau examinations, schedule a closing conference with IS management and prepare the agenda.

9. Notify appropriate attendees (i.e., institution or servicer bureau management, agency manager and staff) of the closing conference location, date, and time.

10. When warranted, inform the CEO that a formal presentation of the examination results should be scheduled for the next meeting of the board of directors.

11. Recommend administrative actions, if appropriate.

12. Complete the preliminary draft of the IS ROE in "camera ready" form and provide copies to the IS

examination manager and safety and soundness EIC on concurrent examinations.

13. Incorporate review comments and forward the ROE to the IS examination manager and safety and soundness EIC.

TIME AND BUDGET

The supervision by risk approach requires the use of examination time-planning techniques, beginning with pre-examination analysis, to more effectively manage and control an examination. Pre-examination analysis is stressed as a way to reduce on-site examination time and enhance the scoping process.

Once the scope is established, the IS EIC or IS manager will establish staffing requirements, time frames, and examiner resource budgets. The IS EIC must record and report all IS examination hours and see that examination objectives are achieved within budget. On-site and off-site hours should be summarized for inclusion in the Administrative section of the ROE.

If preliminary conclusions determine that management controls are lacking in all areas, consideration should be given to suspending or terminating the examination. When time standards prove too short, examiners should forward a request for additional time with justification to their manager.

WORKPAPER GUIDELINES

Workpapers are used to document IS examination procedures and support specific conclusions. They also serve as a reference source during the ROE review process. The IS EIC and IS examiners must organize and index workpapers in a logical and orderly manner. The completeness, accuracy, and clarity of the workpapers also serve as a tool to evaluate the performance of the individual members of the examination team.

Workpapers should be prepared for every area reviewed during the examination. They must provide sufficient documentation for a reviewer (supervising IS examiner, field manager, non-IS examiner, etc.) to understand what was done, why it was done, and how conclusions were reached. A high level index detailing all areas reviewed should be placed at the beginning of the workpapers.

At a minimum, the workpapers for each area should contain:

- An index for each area covered.
- A summary of conclusions and management's response.
- A copy of the conclusions written by the examiner assigned to each area.
- A copy of the completed workprogram section for that area.
- Documents that support each procedure performed.
- Documents that support the specific comments and conclusions of the examiner completing the workprogram section.

Workpapers are the property of the agency and should be secured at all times. The IS examiner may not release examination workpapers or reports to non-agency persons without proper authorization. Exceptions to this rule are joint examinations with other agencies. Copies of workpapers or any internal memoranda should never be released to institution personnel. The IS EIC should contact appropriate agency management for information on disclosure.

The following guidelines should be used to prepare workpapers:

- All workpapers should be titled, dated and identify the institution, examination date, and person responsible for their preparation.
- Workpapers should contain only essential information. Manuals and lengthy policies may be documented by including a copy of the table of contents or cover page for each.
- Items with deficiencies require more documentation.

- Conclusion memos, including operating deficiencies, should be cross-indexed and referenced to applicable workpapers.

- All documents in the workpapers should include an explanation of their relevance to examination results or conclusions.

- Other information may include the EIC information report, copies of the notification and pre-examination letters, a copy of the closing meeting outline, and a list of data center personnel and phone extensions.

Workpapers should be assembled, indexed, and cross-indexed to other workpapers to permit a reviewer to locate work performed (see Workpapers Organization/Format section which follows). All reported comments should be cross-referenced to the conclusion memos filed in the workpapers. All workpapers should be reviewed by the IS EIC prior to leaving the examination site.

WORKPAPERORGANIZATION/FORMAT

In general, the workpapers should be organized into the following sections.

Report of Examination

This section should contain all information relative to the ROE. Only the final version of the IS examination report is filed in the workpapers. The IS EIC should include recap notes of the exit conference and analysis of the adequacy of management's response to the recommendations for corrective action. All information should be filed in chronological order.

IS Examination Scope

This section should contain the IS examination scope memo, cross-referenced to other sections of the workpapers.

Summary of Conclusion Memos

This section should contain the summary of conclusions and accompanying conclusion memos.

Workpapers

This section should be organized in the order of the FFIEC IS Examination Workprogram sections, consistent with the examination scope.

General File (Exhibits)

This section should contain the general information obtained during the pre-examination preparation phase, and any other information gathered during the examination that is not used in the workpapers section. The Exhibits sections should be updated during each examination and obsolete material discarded.

Administrative

The administrative section should contain:

- Information for next examination.

- Examiners' assignment schedule and time control log.

- Correspondence, such as:

  – IS examination notification.
  – Examination request input sheet.
  – Appropriate financial information.
  – Listing of customers for service bureaus.
  – Ratings.
  – Other correspondence, etc.

WORKPAPER REVIEW

The IS EIC reviews examiner workpapers at the institution or service bureau for compliance with the following guidelines:

- Clarity in communicating IS examination objectives and procedures.

- Adequacy in documenting and cross-referencing information used to substantiate reported findings, conclusions, and ratings.

- Completeness and organization of work.

- Unnecessary documents that should be removed.

The IS manager is responsible for reviewing workpapers or delegating that it be done. The review should ensure that the overall quality, competency, and consistency of workpapers is consistent with member agency standards or with the FFIEC.

CONCLUSION MEMOS

As examination procedures are performed, summary notes and conclusions may be written in the "Comments" column of the workprogram or on a separate sheet with the appropriate reference information. IS control deficiencies should be documented in conclusion memos. This should summarize the control objective, important facts and findings, conclusions and, if applicable, recommendations. These items should be discussed with management and its response/corrective action included in the conclusion memos.

Conclusion memo comments should provide clear, concise summaries of problem areas and, when appropriate, recommendations for correction. Results should be substantiated and cross-referenced to supporting information in the workpaper documents. All conclusion memos should be cross-referenced and listed in the Summary of Conclusions.

Conclusion memos should contain:

- Heading Information

  – Name of Institution:
  – Reference Number:
  – Date of Examination:
  – Examiner Initials:
  – Work Program Section:

- Description of Conclusions:

  – *Condition* – The circumstances surrounding the issue should be stated in sufficient detail to permit the reader to understand what was found or what happened and why it is relevant.

  – *Criteria* – If the condition involves a deviation from a law or regulation, it should be identified and relevant portions stated.

  – *Cause* – If the effects are considered significant, the cause of the condition should be stated clearly and concisely.

  – *Effect* – The effects of the condition should be described in sufficient detail to establish their significance (or insignificance) and relationship to the condition.

- Examiner's Recommendations

  Proposed solutions to correct, or reduce the problems should be developed in discussions with management and stated in the recommendations section.

- Management's Response

  The examiner should summarize management's initial response when preparing conclusion memos. However, a written response may be requested for significant findings and conclusions.

After the conclusion memos have been reviewed with and approved by the EIC, discussions with management can be held. Management's response should be summarized and documented, including its opinion on the significance of the concerns and commitment for corrective action.

SUMMARY OF CONCLUSIONS

In preparation for the ROE, a summary of significant examination findings and exceptions, conclusions reached, and management's response and proposed corrective action, if any, is documented in a summary of conclusions document. It is based on the individual workprogram's working paper conclusion memos worksheets that were prepared during the examination. The document should cross-reference individual findings and conclusions comments to the workpapers.

The summary of conclusions form serves as a project management tool for reporting the status of examination findings and conclusions during the examination. Each finding should be cross referenced to the scope memorandum and supporting workpapers. On longer examinations, a copy of the summary of conclusions form containing preliminary information should be updated and made available to the safety and soundness EIC and IS examination manager periodically.

The IS EIC is responsible for the preparation of the summary of conclusions. In addition to current examination findings and conclusions, all unresolved exceptions from the previous examination should also be included. If a deficiency listed in the summary of conclusions is excluded from the ROE, the reasons for doing so must be stated. In addition, appropriate

notations should be made on the report to indicate any changes in the final ROE resulting from management's review.

EXIT CONFERENCE

The objective of the exit conference is to communicate clearly the examiner's findings, conclusions, and recommendations, and to obtain management's commitment to corrective action.

In concurrent examinations, the safety and soundness exit conference, and agenda, are arranged by the safety and soundness EIC. At the end of the IS portion of concurrent examinations, the IS EIC should review the findings and conclusions with the institution's IS management in an exit conference. This may be done in a separate meeting or as part of the safety and soundness exit meeting.

In stand alone institution and service bureau examinations, the IS EIC arranges the exit conference and prepares an agenda letter. The agenda letter should be signed by the appropriate manager and addressed to senior level management, preferably the chief executive officer. The agenda should include the main issues of the draft examination report. Possible attendees may include the chairman of the board of directors, chief executive officer, senior management responsible for IS, the IS examination manager, and other agency examiners. All potential attendees should be informed of the meeting time and location several business days before the meeting date.

Prior to the meeting, the IS EIC should review all material with lower and mid-level management of the institution. All disagreements on factual matters should have been researched and investigated prior to the exit conference. The meeting should never contain any surprises of a factual nature.

BOARD MEETING

In concurrent examinations, the safety and soundness EIC conducts the board meeting. The IS EIC should present the IS findings and conclusions for composite 4 and 5 rated institutions jointly with safety and soundness.

In stand alone institution and service bureau examinations, the IS EIC will present the ROE findings and conclusion at a board meeting for composite 4 and 5 rated institutions. The IS examination manager should attend these meetings as appropriate. The IS examination manager will use judgment in scheduling board presentation for other ratings.

IS ROE FORMAT

The IS report format and instructions contained in the 1996 FFIEC IS Examination Handbook should be used to prepare the IS ROE. (See Chapter 5 for additional information on report format and structure.)

The IS ROE report contains an Open Section which is distributed to the institution or service bureau, and an Administrative Section, which contains information for internal agency use only (see FFIEC issuance SP-1 in Chapter 25 FFIEC Policies for additional information). All significant findings and conclusions of an objective nature, including management comments, should be presented in the Open Section, (i.e., unsafe and unsound practices, noncompliance with statutes and regulations, and deficiencies in computer security and internal controls). Matters that are subjective or considered inappropriate for disclosure to the institution or service bureau being examined should be reported in the "Administrative Section" of the report.

In preparing the final IS ROE, examiners must consider the following and ensure that:

- Findings, conclusions, and comments are adequately communicated and are fully supported by adequate examination work.
- Technical terms, phrases, and acronyms are explained.
- Judgment and discretion are used in presenting findings, examiner conclusions, and concerns.
- Topics and content are organized logically and prioritized appropriately for senior management's attention.

SERVICE PROVIDER REPORT DISTRIBUTION

Upon completion of an IS examination of an independent servicer, distribution will be based upon the policies detailed in FFIEC issuance SP-1 (See Chapter 25 FFIEC Policies for additional information). The final

transmittal letter to the independent servicer's senior management will carry the signature of the appropriate agency personnel and address overall concerns. The ROE will be sent to the independent servicer's board of directors. The member agency initiating the letter will request that the board respond to the report within a specified time period, usually 30 days. For MDPS examinations, the transmittal letter should be approved by the appropriate supervisory office.

A copy of the independent servicer's ROE will be distributed by the IS manager of the authoring agency to involved FFIEC member agencies. Distribution, as authorized/required, will be made to serviced institutions by the responsible supervisory agency. The ROE should not be mailed to institutions until after the service bureau receives their copy of the ROE.

Agency management should track all copies of the independent servicer ROE. The Open Section is the main body of the report and is distributed to both the independent servicer and serviced institutions. The Administrative Section is confidential. Its distribution is limited to member agency management and other regulatory personnel. The report distribution policies and procedures will follow the guidelines contained in the FFIEC IS Examination Handbook.

An examination finding that an MDPS service bureau is in imminent danger of failure (usually a composite 5 rating), or otherwise threatens the safe and sound operations of any member institution, should be discussed promptly with district/regional staff and headquarters to determine the appropriate action.

ENFORCEMENT ACTIONS

Institutions with unfavorable examination ratings are presumed to warrant formal enforcement action. Enforcement actions will be initiated by the responsible member agency in accordance with that agency's internal policies in this area. Independent servicer's with a final composite 4 or 5 IS rating generally will require some type of enforcement action.

IS EXAMINATION RATINGS AND ROE CHAPTER 5

(FILE NAME ON DISK # 1 = S1C5.WPD)

The rating system for data processing operations is similar to the "Uniform Interagency Bank Rating System," which is used for federally regulated financial institutions and is based upon an evaluation of the overall financial institution performance. The IS rating system is explained in FFIEC SP-2 Uniform Interagency Rating System for Data Processing Operations. This policy was issued by the FFIEC and all member agencies in October 1978. This FFIEC SP (Standard Policy) issuance identifies four basic component areas that are common to all IS organizations (see Chapter 25 for additional information). It applies to an organization that maintains an internal IS department or uses a private servicer.

Each data center will be assigned a composite rating based upon the separate component or performance ratings assigned by the IS examiner to the IS functional areas. Each of these functional areas: Audit, Management, Systems Development and Programming, and Operations, will also receive a component rating at every IS examination.

COMPOSITE RATINGS

The composite rating can range from 1 through 5, with 1 representing the best and 5 the worst rating. To arrive at the composite rating, the interrelationships and relative importance of the four functions rated under the component ratings must be considered. Occasionally there will be factors that are not reflected in any specific performance rating, but are important to the data center's overall condition. They should be reflected in the organization's final composite rating. Each composite rating is described as follows:

Composite - 1
Data centers in this group are sound in almost every respect. If deficiencies are noted, they are minor and can be handled routinely and without further supervisory involvement.

Composite - 2
Data centers in this group are 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 experience a combination of adverse factors that 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 is such as to make operation failure only a remote possibility.

Composite - 4
Data centers in this group are operating under unacceptable conditions that could impair future viability. A high potential for operational and/or financial failure is present. Still 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 that are pronounced to a point that threatens the ultimate continuation of the operation. Immediate affirmative action and continuous supervision, as required by the regulator, are necessary.

COMPONENT RATINGS DEFINITIONS

Each performance or component rating also ranges from 1 through 5, with 1 representing the highest and 5 the lowest rating. Each functional area of activity (Audit, Management, Systems Development and Programming, and Operations) must be evaluated to determine its individual performance rating.

Each performance or component rating is described as follows:

Component - 1 – Strong performance
Performance that is significantly higher than average.

Component - 2 – Satisfactory performance
Performance that is average or slightly above and that provides adequately for the safe and sound operation of the data center.

Component - 3 – Fair performance
Performance that is somewhat flawed and is considered to be of below average quality.

Component - 4 – Unsatisfactory performance
Performance that is significantly below average and, if left unchecked, might evolve into weaknesses or conditions that could threaten the integrity of the records processed and the viability of the institution or data center.

Component - 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.

COMPONENT RATING AREAS OF COVERAGE

Audit – is rated (1 through 5) for:

- Audit overview
  - Audit effect positive change to reduce risk
  - Adequate audit coverage (timely/competent)
  - Based on complete universe
- Audit Organization
  - Independence
  - Board of directors' support
  - Resources allocated
  - Management and staff succession
- Audit Staffing
  - Adequacy
  - Qualifications
  - Training
- Internal/External Audit Activities
  - Quality of audits scope
  - Frequency
  - Standards and procedures
    - Adequacy and
    - Compliance
  - Follow-up and correction of exceptions
  - Working papers and documentation
    - Completeness
    - Security
  - Audit software
    - Use
    - Effectiveness
    - Documentation
  - Audit reports

Management – is rated (1 through 5) for:

- Effectiveness of Management
  - Organization
  - Resources allocated
  - Leadership
  - Administrative abilities
  - Qualifications
  - Delegation of responsibilities
  - Support
  - Management succession
- Correction of Deficiencies
- Compliance Performance
  - Laws and regulations
  - Awareness
  - Compliance
  - Contracts
- Planning and Direction
  - Planning
    - Strategic (longer term of 3 - 5 years)
    - Tactical (shorter term of 1 - 2 years)
    - Operational (less than 1 year)
  - Risk analysis
  - User involvement
  - Senior management involvement
  - Budget
- Corporate Information Security Program
  - Enterprise-wide basis
  - Mission statement developed
  - Formal awareness program
  - Status and health of program
- Corporate Contingency Planning
  - Enterprise-wide basis

User/functional departmental basis
Appropriate integration of IS D/R planning
Status and health of program

- Standards and Procedures
  Development
  Enforcement

- Internal Controls
  Development
  Enforcement

- Physical Security
  Development
  Enforcement

- Adequacy of MIS
  Senior management/board level
  Departmental level
  Timely, accurate, consistent, and relevant

- Financial Condition

Systems Development and Programming – is rated (1 through 5) for:

- S&P Organization
  Separation of duties
  Resources allocated
  Management and staff succession

- Staffing
  Adequacy
  Qualifications
  Training

- Standards and Procedures
  Adequacy
  Compliance
  User liaison

- Documentation
  Completeness
  Organization
  Storage and security

- Internal Controls
  Modification and change procedures authorization, documentation, and implementation
  Program library maintenance
  Systems development

- Physical Security
  Documentation
  Software
  On-line systems

Operations – is rated (1 through 5) for:

- Operations organization
  Separation of duties
  Resources allocated
  Management and staffing succession

- Staffing
  Adequacy
  Qualifications
  Training

- Standards and Procedures
  Adequacy
  Compliance
  User liaison

- Operations
  Processing concerns:
  - Data entry control
  - Processing controls
  - Output distribution controls
  - Security - physical and data
  - Emergency planning
  - Data center disaster/recovery planning
  - User communication

  Operations Activities:
  - Networking
  - End-user computing
  - Document Imaging
  - EFT activities - wholesale, retail, ACH
  - IS servicing as provider and receiver

The overall order of the Supervisory Tools section of this Handbook list the narrative chapters and their related workprograms as they would appear in the component rating categories.

COMPONENT	RATING	RELATIONSHIPS
Primary Component Rating Area	**Chapter Number Reference**	**Related Handbook Chapters**
Audit	8	Internal/External Audit
Management	9	Management
	10	Corporate Contingency Planning
	11	MIS Review
Systems and Programmin g	12	Systems Development and Programming
Operations	13	Operations
	14	Security - Physical and Data
	15	Networking - Client/Server
	16	End User Computing
	17	Document Imaging
	18-21	EFT Chapters (4)
Other	22	IS Servicing - Provider/Receiver[1]

[1] If findings are related to IS Servicing - Provider/ Receiver, they should be addressed in this component rating section that most closely relates to the nature of the finding.

FFIEC IS ROE INTRODUCTION

A uniform IS report of examination (ROE) format has been approved by the FFIEC to report the results of IS examinations.

The standard IS examination report format provides for:

- Standardized reporting for both financial institutions and service bureaus.
- Enhanced coordination among FFIEC member agencies.
- The regulatory oversight needs of FFIEC agency supervisory and management personnel.

GUIDELINES FOR COMPLETING

Each FFIEC agency may supplement the following guidelines with additional instructions. All required sections, however, must be completed for reports to be used on an interagency basis.

All FFIEC IS examination reports have two sections. The open section, which is distributed to examined entities and an administrative section, which is confidential and for regulatory agency use only. The open section of service bureau reports may also be distributed to the regulated financial institutions that are service bureau customers.

SECTIONS OF ROE

All significant matters of an objective nature should be presented in the open section.

Matters of a proprietary nature should not be included in the open section of service bureau reports. Examples of proprietary information include, but are not limited to, marketing plans, development plans, and certain contract terms.

Subjective matters should be placed in the administrative section of the report.

Correspondence, other than the service bureau examination report, should be used to:

- Transmit ratings to service bureau boards of directors.
- Remind serviced institution management periodically of their continuing responsibility to assess regularly how the institution needs are being met by a service bureau.

OPEN SECTION – REQUIRED AND OPTIONAL PAGES

Cover Page (Required)

Interagency reports of examination should use the standard interagency cover page. Each agency has the option of using either its own cover page or the standard FFIEC cover page on its institution's examinations.

Table of Contents (Optional)

The use of this page depends upon the complexity and length of the report and on the degree to which the presentation of the examination findings will be enhanced by its inclusion. When used, major sections should be listed in order of their appearance in the report.

Examiner's Conclusions (Required)

Information should include:

- Scope and Objectives of the Examination – A description of areas examined and procedures employed. The limitation, waiver, or expansion of certain examination areas should be noted and fully explained.

- Summary of Major Findings – A general description of major examination findings. The findings should be presented in order of their importance. (All findings NOT included in the summary should be identified on a separate listing and left by the examiners with management.) References to areas where significant operational and procedural deficiencies or internal control weaknesses were observed should be included. The reader should be referred to the specific "Supporting Comments" page(s) for detailed descriptions of these deficiencies and recommendations for corrective action.

  The last paragraph should list senior level management with whom the examination findings were discussed. The list should be limited to those persons with broad responsibility for the major areas examined, i.e., audit, systems and programming, and operations. Senior management responsible for information systems operations should always be included.

  Comments in the summary section should be directed to the attention of the board of directors and senior management and should be brief, non-technical, and limited to the most significant issues. Describe the findings in terms of the risk(s) presented and potential effect on the organization and its customers.

- Conclusions – Present a summary of the overall condition of the information systems examined, including comments on the improvement or deterioration of the operation. Avoid single-word evaluations, such as good, fair, poor, strong, or weak. The summary should include, as appropriate, brief comments about past performance (with emphasis on effecting corrective measures), the seriousness of existing weaknesses, and future prospects for the information system. Also include information on any corrective action that management has indicated will be undertaken.

- Composite Rating – These remarks should document the performance evaluation of the entity in accordance with FFIEC's SP-2 Uniform Interagency Rating System for Data Processing Operations. Following the numerical composite rating, the exact language for that rating in FFIEC SP-2 should be inserted, so that the board members and management have a clear and common understanding of the examiner's overall conclusions. Supporting comments should preceed the composite rating in this section of the report.

  Note: The composite rating for organizations that service regulated entities should not be disclosed to, or discussed with, the serviced federally insured financial institutions. It should be communicated in the examination report transmittal letter. The composite rating for examinations of institutions not servicing other regulated entities should be disclosed in the Conclusions section.

- Signatures – The authoring EIC must sign the report at the bottom of the "Examiner's Conclusions" page. Other signatures required by the authorizing agency should follow and include appropriate titles.

Violations of Laws and Regulations (Optional)

This page should be completed whenever specific violations of laws or regulations are discovered during an examination. Comments should cite the law(s) or regulation(s) violated followed by a brief description of the violation and management's response about corrective measures.

Supporting Comments (Required)

Operating and procedural deficiencies and internal control weaknesses identified during the examination should be discussed in this section. Detailed comments should be presented to support the findings cited in the Examiner's Conclusions section. Supporting comments should be listed in the order of relative importance consistent with the Examiner's Conclusions page. Individual comments should, at a minimum, include:

- A detailed description of the deficiency, identifying the risk to the organization if not addressed by management.
- Examiner's recommendation to address the deficiency.
- Management's response and corrective action plan.
- The examiner's analysis of management's response (if necessary).

The findings must be described in terms of the risks they present and their effect on the organization and its customers.

Every effort should be made to obtain management's commitment to a reasonable time frame for implementing corrective measures. Deficiencies noted in consecutive examinations should be highlighted and given priority. If a significant number of repeat deficiencies are noted, this information should be reported in the Examiner's Conclusions section of the report and should be commented upon in the management section of the report.

Note: Only substantive items should be presented in the Supporting Comments section. Less significant exceptions and weaknesses should be discussed with management and, if appropriate, listed separately to be given to management at the completion of the examination. Such a list should be referenced in these pages or in the "Examiner's Conclusions" section, and a copy should be retained in the workpapers.

Director's Signature Page (Required)

This page should be included in all IS ROEs. Once the final ROE is returned to the institution's directors they should be instructed in the transmittal letter sent by the supervisory agency to fully review the IS ROE at a following board of directors meeting. Once this review has occurred, the directors must sign the *Director's Signature Page* to attest to the fact that each of them have personally reviewed and understand the contents of the IS ROE. They should date their signature to indicate the date of their review.

ADMINISTRATIVE SECTION – REQUIRED AND OPTIONAL PAGES

Only matters that are subjective or considered inappropriate for disclosure in the open section of the examination report should be presented in this section. In addition, financial data should be included for all service bureaus. Basic information about the entity being examined, the type of examination, and the participating supervisory agencies should also be included in the administrative section. Most of the items are self-explanatory. The "Type of Examination-Agency" subsection should indicate whether the examination is joint or rotated and the authoring agency identified by the appropriate abbreviation, (e.g., FDIC, FRB, NCUA, OCC, OTS.) In non interagency examinations, the authoring agency should be identified first and followed by any other information required by individual agency policies. For multisite examinations, hours for all data centers should be included in the corporate report and in the individual subsidiary reports.

Administrative Remarks (Required)

These remarks should document the performance evaluation of the entity in accordance with FFIEC's SP - 2 Uniform Interagency Rating System for Data

Processing Operations. Each numeric rating should be substantiated by brief narrative comments. For multisite examinations, all subsidiary data center ratings should be included in this section and summarized.

Comments should convey a clear assessment of the condition of each function as well as the overall condition of the information systems operation. They should not merely restate the conclusion from the "Examiner's Conclusions" page(s). The numeric ratings and accompanying comments should include recommendations for follow-up action and additional subjective comments.

Statistical Data (Required)

This page(s) should contain statistical information necessary to supervise the institution/ service bureau adequately and process the report. This information should be requested at or before the beginning of the examination. Instructions for completing various pages include:

- Applications – Present a list of the major applications processed by the service bureau for itself and for serviced financial institutions that are federally insured. The applications should be numbered sequentially, i.e., 1, 2, 3, 4, and typed under the heading "Code." The sequence number will serve as a key for the "Serviced Financial Institutions" portion. The "Application" portion should indicate the processing mode(s) for each application listed. The modes are defined as:

  - *Batch updating* – Daily transactions activity is accumulated off-line and is run once at the end of the processing cycle (usually daily) to update the customer master files.

  - *Memo post/On-line updating* – Transaction activity against customer master files are accumulated during the day on the system and actual updating of the customer master file records occurs at a later scheduled time during that processing cycle.

  - *Real-time updating* – Transactions are posted to the data files as they occur. Customer files are updated in place.

  Note: If appropriate indicate the combinations of these processing modes.

- Serviced Financial Institutions – List names and locations of federally insured serviced financial institutions. The list should be grouped by regulatory category, i.e., national banks, state member banks, state nonmember banks, savings and loan associations, and credit unions. This listing can either be included in the IS ROE or transmitted separately.
  Applications processed should be identified in the right-hand columns, using the keys assigned in the application section. (This information may also be provided as a separate attachment to the administrative section of the examination.)

Other Servicing (Required)

- Other Servicing – At a minimum, include the number of customers omitted from the previous categories and the types of processing performed for these organizations.

- System Description – Provide details of the major hardware, software and, if applicable, teleprocessing configurations used by the facility.

  - *Hardware* – At a minimum, specify the manufacturer, model number, and core storage capacity of the mainframe used. Detail other information as appropriate or as required by the individual agencies.

  - *Software* – Indicate the primary programming languages used and the major sources of software, e.g., developed in-house, software packages, contract programmers. If software packages are used indicate from whom packages were purchased.

  - *Networking/Teleprocessing* – If networks are used, indicate the general configuration of the system, specifying remote entry sites, free standing satellite centers, and the number of terminals.

- Organizational Structure – Provide general staffing and examination contact information. Also, list principal officers and managers responsible for the center's operation by name, title, and phone number. If the organization is a

financial institution, provide total asset and deposit figures. The type and name of the organization should be specified on the ownership portion of this section. Types of organization might include financial institution (bank, S&L, or credit union), financial institution or holding company subsidiary, bank service corporation, private corporation, joint-venture, facilities management (specify contracting financial institution), partnership, etc. If the organization is not a financial institution, the major owners and directors should be listed.

Financial Data (Required for all Service Bureaus)

This page should be completed for all service bureaus that are not financial institutions. Data should be included for the last three fiscal years.

Audited financial statements should be requested. If they are not available, unaudited statements will be acceptable. If interim statements are obtained, they should be detailed on a separate page, footnoted to indicate that they are interim statements, and inserted behind the year-end statements.

Significant footnotes in the financial statements should be summarized on a blank insert page and included at the end of the financial data.

If the servicer is part of a regulated financial organization, the examiner should use existing regulatory financial and analytical information (CAMEL rating, BOPEC rating, MACRO rating, etc.), in the review and analysis of the parent company.

If the service bureau is a subsidiary of a nonbank holding company or other nonfinancial corporation, both consolidated and company financial statements should be requested and analyzed by the examiner. Consolidated statements should be detailed on separate pages, footnoted to indicate they are consolidated statements and inserted after the company year-end and interim statements.

Additional Information (Optional)

This page is provided to address specific requirements of the various regulatory agencies. Information included would be items such as the location of workpapers and reports requested to support safety and soundness or compliance examinations.

In-house Examinations vs. Service Bureau Examinations

The examiner should be aware that there are differences between the format used for in-house examinations and that used for Service Bureau examinations. The basic differences are:

- Cover page(s).
- Rating disclosure.
- Financial Analysis.

The cover page(s) will differ among agencies, so refer to the appropriate agency policies. If a joint examination, the cover page(s) used will be that of the lead agency.

The attachments that follow may be used as an example of a report of examination. It should be noted that the cover page(s) are standard and required, even though each agency may have slightly different wording. The other pages are examples only and may be changed to conform to each agency's policies.

A sample of each required and optional page for the FFIEC IS ROE follows.

FFIEC INFORMATION SYSTEMS

REPORT OF EXAMINATION

[Fin. Inst. or Servicer]

[City] [County] [State]

Examination Date: [Examination Date]

PARTICIPATING AGENCIES

AGENCY	REGION/DISTRICT
[Agency]	[Region/District]

Examiner(s): [Examiner-In-Charge]

THIS REPORT OF EXAMINATION IS STRICTLY CONFIDENTIAL

This copy of the examination report is the joint property of the above regulatory agencies and is furnished to the data center for its confidential use. The information contained in this document is based upon the records and books of the center, upon statements made by the directors, officers, and employees, and upon information obtained from other sources believed to be reliable and correct.

This examination is not an audit and should not be construed as such. It does not replace, nor relieve management of its responsibility for making or providing for adequate audits of the center.

Under no circumstances shall any recipient of this report, or any of its directors, officers, employees, attorneys or auditors disclose or make public this report or any portion thereof. The law provides penalties for unauthorized disclosure of any of the contents of this report. If a subpoena or other legal process is received calling for the production of this report, the office of the agency that transmitted this report must be notified immediately.

TABLE OF CONTENTS

EXAMINER'S CONCLUSIONS

References

INTRODUCTION . . . . . .

PURPOSE . . . . . .

SCOPE AND OBJECTIVES OF EXAMINATION . . . . . .

REPORT DISCUSSION . . . . . .

SUMMARY OF MAJOR FINDINGS . . . . . .

CONCLUSION . . . . . .

COMPOSITE IS RATING . . . . . .

SUPPORTING COMMENTS . . . . . .

- **INTERNAL/EXTERNAL AUDIT** . . . . . .
- **MANAGEMENT** . . . . . .
- **SYSTEMS AND PROGRAMMING** . . . . . .
- **OPERATIONS** . . . . . .

SIGNATURES OF DIRECTORS . . . . . .

EXAMINER'S CONCLUSIONS

EXAMINER'S CONCLUSIONS (Continued)

Agency Examiner-in-Charge

Agency Director

VIOLATIONS OF LAWS AND REGULATIONS

SUPPORTING COMMENTS

SIGNATURES OF DIRECTORS

We the undersigned directors of [INSTITUTION NAME] have personally reviewed the contents of the Report of Examination dated [EXAM DATE].

Signatures of Directors	Date

NOTE: This form should remain attached to the Report of Examination an d be retained in the institution's file for review du subsequent examinations. The signatures of committee members will suffice only if the committee includes outside direc and a resolution has been passed by the full board delegating the review to such committee.

ID No.

ADMINISTRATIVE SECTION

Region/District:	ID Number:

Name & Location of Institution

Examination Opened	Examination Closed	Type of Examination - Agency

Prior Exams:

Date:	Rating:	Agency:	Date:	Rating:	Agency:

EXAMINERS	Level	Working Hours		
		In Center	Outside	Total
	TOTAL	0	0	0

ADMINISTRATIVE REMARKS

ADMINISTRATIVE REMARKS (Continued)

ADMINISTRATIVE SECTION (Continued)

Region/District:		ID Number:		
		Working Hours		
EXAMINERS	Level	In Center	Outside	Total
	TOTAL	0	0	0

STATISTICAL DATA

Applications				
Code	Application	Batch	On-Line	Real Time

X = All Processing I = Inquiry Only M = Memo Posting F = File Maintenance

STATISTICAL DATA (Continued)

Serviced Financial Institutions													
	Application (By Code)												
Name and Location													

OTHER SERVICING

Number of Customers:

Applications Processed:

System Description

Hardware:

Software:

Teleprocessing:

Organizational Structure

Staff Size: Operations _____ S & P _____ Total _____

Examination Contact:

Officers/Managers:

If financial institution, give total assets: Total Deposits:

Ownership:

Type here.

Directors:

Type here.

FINANCIAL DATA

Condensed Balance Sheet for Nonfinancial Institution Servicer.

CONDENSED BALANCE SHEET As of

	19XX	19XX	19XX	19XX
ASSETS				
Cash				
Accounts Receivable				
Prepaid Expenses				
Other Current Assets				
CURRENT ASSETS	0	0	0	0
Real Estate				
Furniture & Fixtures				
Software				
Software Amortization				
Hardware				
Hardware Depreciation				
Goodwill				
Other Assets				
TOTAL ASSETS	0	0	0	0
LIABILITIES AND CAPITAL				
Notes Payable Banks				
Notes Payable Others				
Accounts Payable				
Accrued Expenses				
Taxes				
Other Current Liabilities				
CURRENT LIABILITIES	0	0	0	0
Term Debt				
Other Debt				
Subordinated Debt				
Long-Term Capital Leases				
TOTAL LIABILITIES	0	0	0	0
EQUITY CAPITAL	0	0	0	0
TOTAL LIABILITIES & EQUITY CAPITAL	0	0	0	0

000's Omitted.

FINANCIAL DATA (Continued)

Condensed Income Statement for Nonfinancial Institution Servicer.

CONDENSED INCOME STATEMENT As of

	19XX	19XX	19XX	19XX
OPERATING INCOME				
Data Processing Servicing Income				
Other Income				
TOTAL OPERATING INCOME	0	0	0	
OPERATING EXPENSES				
Mainframe Hardware and Software:				
Lease and Rental				
Depreciation				
Repairs and Maintenance				
Contract Programming				
License Fees and Amortization				
Other				
Other Operating Expenses:				
Compensation				
Data Communication				
Occupancy Expense				
Benefits and Travel				
Public Relations & Advertising				
Other Operating Expenses				
TOTAL OPERATING EXPENSES	0	0	0	
NON-OPERATING				
Non-operating Income:				
Interest Income				
Other Non-operating Income				
Non-operating Expenses:				
Interest Expense				
Other Non-operating Expenses				
NET NON-OPERATING INCOME	0	0	0	
INCOME BEFORE TAXES	0	0	0	
Applicable Income Taxes				
NET INCOME BEFORE EXTRAORDINARY ITEMS	0	0	0	
Extraordinary Credits (Charges)				
NET INCOME	0	0	0	

000's Omitted.

FINANCIAL DATA (Continued)

SUMMARY OF KEY OPERATING RATIOS

	19XX	19XX	19XX	19XX
Asset Growth				
Liability Growth				
Capital/Total Assets				
Return on Assets				
Return on Equity				
Net Operating Income/ Gross Operating Income				
Current Assets/Assets				
Debt/Equity				
Current Assets/Current Liabilities				

OPERATING RATIO DEFINITIONS

1 **Asset Growth**
(Current Total Assets - Prior Period Total Assets)/Prior Period Total Assets
A significant increase or decrease in total assets may be an indication of problems and should be investigated and explained.

2 **Liability Growth**
(Current Total Liabilities - Prior Period Total Liabilities)/Prior Period Total Liabilities
A significant increase in Total Liabilities is a potential indication of cash flow problems and should be investigated and explained.

3 **Capital/Total Assets**
Equity Capital/Total Assets
This ratio provides an indication of the amount of losses that can be absorbed before insolvency.

4 **Return on Assets**
Current Period Net Income/((Current Period Total Assets + Prior Period Total Assets)/2)*
Return on Assets is an indication of how efficiently the assets are being used.

5 **Return on Equity**
Current Period Net Income/((Current Period Equity + Prior Period Total Equity)/2)*
An indication of the return on the capital invested.

6 **Net Operating Income/Gross Operating Income**
An indication of the efficiency of the operation.

7 **Current Assets/Assets**
An indication of liquidity.

8 **Debt/Equity**
Long-term Debt/Equity Capital
An indication of liquidity.

9 **Current Assets/Current Liabilities**
An indication of liquidity.

* This ratio should be annualized if current period less than 12 months.

ADDITIONAL INFORMATION

MULTIREGIONAL DATA PROCESSING SERVICER PROGRAM (MDPS)

CHAPTER 6

(FILE NAME ON DISK # 1 = S1C6.WPD)

Large multiregional data processing servicers (MDPS) with data centers located in different geographic regions pose a systemic risk to the financial industry should one or more fail. Since these companies service banks, thrifts and credit unions, the FFIEC Task Force on Supervision has determined that it is more effective and efficient to conduct one interagency IS examination of large servicers instead of several separate data center examinations by different member agencies. Interagency IS examinations provide a single examination report for the servicer management and the board of directors. The program also facilitates better communication among regulatory agencies and servicer management.

An organization is considered for the MDPS program when it processes:

- Major applications for a large number of financial institutions that are regulated by more than one agency thereby posing a high degree of systemic risk.
- Work from a number of data centers located in different geographic regions. Generally, the total assets serviced are more than $20 billion.

Prior to September 30 each year, the FFIEC IS Subcommittee of the Task Force on Supervision publishes a schedule of MDPS examinations designating the servicer, the date of the examination, and the lead agency for the following year(s). This schedule is distributed by the IS Subcommittee agency representatives to their respective regional/district offices.

The following MDPS examination guidelines supplement the policies and procedures contained in the FFIEC SP-1: Interagency IS Examination, Scheduling and Distribution Policy (See Chapter 25 for additional information).

RESPONSIBILITIES OF LEAD AGENCIES

A lead agency is selected for each MDPS examination by the FFIEC IS Subcommittee. It administers the MDPS examination on behalf of all participant FFIEC member agencies. The MDPS program represents a cooperative arrangement among member agencies for the achievement of shared common supervisory goals and objectives. All member agencies participate in key decisions on MDPS examinations through the FFIEC IS Subcommittee. For example, involved member agencies participate in the selection of vendors entering/leaving the MDPS program, approval of the supervisory strategy and scheduling of examinations, selection of sites for examination, and involvement in key meetings with management and the boards of directors. The lead agency will normally conduct two consecutive examinations, after which the "lead" will rotate to another agency. The FFIEC member agency selected as the lead agency generally will assign the responsibility for the examination to the appropriate district/regional office in which the servicer headquarters is located.

The MDPS EIC is responsible for including the requirements of participating agencies in the supervisory strategy and scope of supervisory activities, leading the on-site examination, assigning the ratings, writing the ROE, and communicating the status of the examination to participating agencies and follow-up. As overall lead of the examination, the MDPS EIC must work closely and communicate frequently with appropriate representatives of participating agencies including Washington, district/region, and field personnel. The FFIEC IS Subcommittee is responsible for providing direction and guidance to the overall MDPS program.

The lead agency assigns the EIC for the MDPS examination (MDPS EIC). Lead agencies should coordinate staffing assignments with the agency that is expected to head the next examination. This ensures that the MDPS EIC for the next examination is familiar with the entire MDPS operation by participating in the current

examination. The MDPS EIC must identify risk, prepare the supervisory strategy, set the scope of the examination, assign the ratings, write the ROE, and communicate the status of the examination to participating agencies.

GENERAL PROCEDURES

Frequency of MDPS Examinations

The frequency of examinations for MDPS data centers is the same as that listed for supervised service bureaus. Their ongoing condition should be monitored between examinations through periodic visitations and progress reports. This information should be coordinated with the FFIEC IS Subcommittee.

Pre-Examination Procedures

The pre-examination review is conducted by the MDPS EIC to determine the scope of the overall examination, identify resource requirements, schedule events, and determine the data centers to be examined. At a minimum, the pre-examination scope document should provide details on the organization's corporate history, corporate and organizational structure, scope of the upcoming examination, data centers included in the examinations, and examiner requirements.

The pre-examination review may include meetings with MDPS management to discuss changes that have taken place since the prior examination, or that may occur in the near future. The appropriate agency's Washington office should be informed of any problems serviced institutions may experience with an MDPS servicer.

Scope of Examination

The MDPS EIC develops the scope of the examination during the pre-examination review and selects the data centers to be examined. Findings from data centers operating under a facilities management contract should be considered in the examination findings, but not included in the ROE. The scope document for all MDPS examinations is presented by the lead agency's Washington office to the FFIEC IS Subcommittee for approval.

The scope document should be completed by the lead agency at least 90 days prior to the target date for the headquarters examination, except when a 120-day lead time is requested, because of the size and complexity of the examination. The agency's Washington office will distribute the examination scope document to the other regulatory agencies.

Time Frames

The MDPS EIC sets the time frames for examining the data centers and for the submission of reports. Subsidiary data center examinations should generally not begin more than 60 days prior to the target date of the headquarters examination. The completed reports should be submitted to the MDPS EIC for consolidation prior to the start of the headquarters examination.

Presentation of Findings and Recommendations

The MDPS EIC will notify agency Washington office staff of the date, time, and location of the presentation of examination findings and recommendations to management of the MDPS. Each participating agency will be able to review the examination findings and be represented at the presentation. However, the number of participants at the presentation may be limited by the lead agency.

Normally, MDPS examination findings are presented first to senior management and then to the board of directors. The agency in charge of the examination should allow senior management and the board a maximum of 45 days to respond following their receipt of the ROE.

Workpapers and Workprograms

Workpapers and workprograms will be retained in the respective offices of the MDPS EIC and lead examiners for servicer data centers. The lead examiner for each data center must review work papers to ensure that the examination findings are accurate and well documented. The MDPS EIC is responsible for the preparation and accuracy of the MDPS examination report.

REPORT PREPARATION AND DISTRIBUTION

Report Preparation

A consolidated report of examination will be prepared by the lead agency. The report should give an overall view of the organization and not each individual data center comprising the MDPS. However, the relative strength of each data center should be evaluated and rated. The ROE should contain an assessment of the major risks to the institutions serviced by the MDPS organization, recommendations for reducing or eliminating those risks, and management's responses to the findings and recommendations. The ROE should be prepared following the guidelines in this Handbook (See Chapter 5 for additional infor-mation). A list of serviced institutions should be included in the administrative section.

The subsidiary data center examination reports should be summarized and consolidated in the corresponding sections of the final report. A separate subsidiary data center report may be issued with the approval of the MDPS EIC, lead agency, and other regulatory agencies. Deviations from the consolidated report format should be approved by the agency's Washington office and by the other participating FFIEC member agencies.

Rating

Each MDPS examination will be assigned one set of performance ratings and one composite rating based upon the overall condition of its entire operation. The MDPS ratings will follow the Uniform Interagency Rating System - FFIEC SP-2 (See Chapters 5 and 25 for additional information). Each MDPS subsidiary data center requires a separate rating. These ratings are not reported in the open section of the MDPS ROE; however, they are included in the administrative section.

Recommendations

At the end of the examination, the MDPS EIC will provide recommendations on resource requirements and the scope of subsequent examinations. These recommendations will assist in planning future MDPS examinations.

Distribution

The lead agency's Washington staff distributes the final MDPS report of examination. The MDPS consolidated report should be sent to the appropriate Washington office for review prior to its distribution. The final MDPS report is distributed to the board of directors of the servicer by the Washington office. The report is also distributed to the FFIEC IS Subcommittee members for distribution to their respective agency district/regional offices. Some agency policies also call for further distribution to appropriate state supervisory agencies and serviced financial institutions.

SHARED APPLICATION SOFTWARE REVIEW PROGRAM

CHAPTER 7

(FILE NAME ON DISK # 1 = S1C7.WPD)

The SASR Program was established in 1990 by the FFIEC IS Subcommittee and is structured similarly to the successful interagency sponsored Shared National Credit Program (SNC). Under SNC large multinational/ regional credit lines, with participation across interagency jurisdictions, are reviewed by interagency groups of credit review examiners annually. In the same fashion, interagency IS examiner resources are used to review and evaluate uniformly the control structure of major software packages used by a wide segment of financial institutions. Normally, a software/turnkey program or system would be used by financial institutions across agency supervisory jurisdictions, leading to cross-agency involvement.

The scope of the SASR program covers: turnkey systems (which generally include an integrated mix of both software and hardware), stand-alone custom software (which runs on a commercially standard hardware configuration), and integrated packages. Criteria for selection includes purchased software that involves high risk applications. These applications were envisioned to include wire transfer, securities transfer, loans, deposits, and general ledger.

SASR PROGRAM

The FFIEC IS Subcommittee believes the primary focus of the SASR program is the review of turnkey software packages used by financial institutions. The benefits of the program include:

- A more cost effective use of agency/interagency IS examiner resources.
- Providing agencies with the expertise to review these systems and applications jointly.
- The ability of each agency to use non-speciality more junior safety and soundness examiners or newer IS examiners who understand a community bank's IS related operational and internal controls. (These examiners generally are not trained to evaluate systems development and programming activities. However, a well-documented SASR report will provide examiners with guidance and assistance to evaluate the small bank IS environment.)

The use of SASR is not limited to the review of community financial institution turnkey systems. It can also be used to support interagency safety and soundness initiatives when focusing on higher risk applications in larger financial institutions. It may be used to evaluate financial institution software packages for wire transfer, capital markets, derivatives development/recordkeeping, securities transfer, and trust transactions.

OBJECTIVES

The SASR program is intended to:

- Augment the IS work in community banks, particularly in systems development and programming.
- Communicate an evaluation that can be used to reduce time and resources needed to examine turnkey facilities.
- Reach conclusions on the adequacy of the software product and whether it is safe, sound, and appropriate for use in a large group of financial institutions.
- Consider systemic risk by targeting software used by a large number of covered financial institutions.
- Maintain a continuing knowledge of software upgrades and changes.

RESPONSIBILITY

The IS Subcommittee of the FFIEC's Task Force on Supervision is responsible ultimately for overseeing the SASR program. This includes choosing software systems for review and selection by the lead agency. Because of the continuing demand by all agencies for senior IS examiner resources, the performance of SASR evaluations must be clearly beneficial when comparing the costs with the benefits.

ADMINISTRATION

The selection of candidates for this program are turnkey

(complete software and hardware systems), stand alone software, and integrated packages. Criteria for selection also includes purchased software that involves high risk applications. Such applications include wire transfer, securities transfer, loans, deposits, and general ledger.

The IS Subcommittee of the FFIEC's Task Force on Supervision oversees the program and selects the software system for lead agency review.

A designated lead agency conducts the review in an institution that it supervises. The review should be preceded by the regular IS examination to ensure that the institution is fully prepared for the review team.
The lead agency also performs:

- Examiner-in-Charge Selection – An experienced IS examiner should be selected to head the review.

- Notification – The lead agency must provide other agencies with at least six months prior notice of the upcoming review to assure the availability of senior IS examiners.

- Research – The lead agency must perform preliminary research of the selected software product before beginning the review. The research information must include background data and a description of the organizational structure of the firm and any user group activity. Information collected before the review aids in setting its scope. (An Examiner Checklist is included with this material.)

- Institution Selection – The lead agency selects the institution where the software review will be conducted and notifies the participating agencies of the target review date. (The institution should use all core software applications.)

- Vendor Notification – The lead agency must notify the vendor of the upcoming software review and to designate a contact person. (See sample letters attached.) The vendor may provide information and suggestions that enhance the review. The vendor must be informed that the final product of this review will be a confidential report for regulatory purposes only. A copy of the report will <u>not</u> be made available to either the vendor or any of the user financial institutions. The vendor should be advised that participation in the SASR program should not be publicized and the review should not be construed as an endorsement of the software program.

- Performance Review – The program administration and instruction documents establish guidelines for performing shared application software reviews. The EIC will advise the financial institution and the software vendor that the SASR is intended to provide an in-depth review of the characteristics and features of a particular software product. A confidential report, summarizing the review findings, must be completed for all such reviews and be strictly for regulatory purposes only. No copies will be provided to the financial institution or the software vendor.

- Exit Meeting – An exit meeting must be conducted at the mutual convenience of the vendor and the participating examiners. Ideally a draft report should be available for this meeting with the vendor. The draft report may be discussed with the vendor representative, but must be returned after the meeting to ensure the accuracy of the information developed. In addition, the EIC may request comments on planned enhancements to the software program.

  Significant areas of concern to examiners identified in the review should be discussed during the exit meeting. With the approval of the IS Subcommittee, they may be documented in a follow-up letter to the vendor. If a meeting is impractical, a conference call will suffice.

- Review Submission – All reviews should be completed and forwarded to the Washington, D.C. office of the lead agency within 30 days from the completion of the on-site review. To facilitate the review process, both a hard copy and an electronic version (preferably ASCII) of the review should be provided.

- Document Review and Distribution -- The IS Subcommittee will review and distribute the final product. Each agency will distribute the report to its respective regional office or district. (These documents are for internal agency purposes only.)

Follow-up – The vendor should be requested to keep the lead agency apprised of major software changes and enhancements.

Scheduled Updates – Feedback from field examiners can trigger another review. These events may include a change of ownership, significant software changes, or new developments that adversely affect institutions using the software.

GUIDELINES FOR SASR REPORTS

These guidelines are provided to assist the examiner in conducting Shared Application Software Reviews (SASR). They address the same areas as the FFIEC IS Workprogram. The examiner may review other areas

based on the findings. Additionally, the examiner is encouraged to include any relevant information obtained from outside sources. This information should be verified.

The SASR is intended to produce a report documenting the characteristics and features of the selected software product. This will assist examiners in conducting examinations (safety and soundness, compliance, bank holding company inspections and IS) of financial institutions using a specific software product. The scope of the SASR should be flexible to accommodate the changing data processing environment and include, at a minimum, the following information.

A cover sheet should clearly state:

- "SHARED APPLICATION SOFTWARE REVIEW."
- Vendor name and corporate address.
- Software product reviewed.
- "THIS REVIEW IS THE PROPERTY OF THE FFIEC MEMBER AGENCIES AND IS NOT TO BE DUPLICATED WITHOUT PERMISSION. THIS REVIEW IS FOR INTERNAL USE ONLY."

A table of contents should be included.

GENERAL OVERVIEW

Page one of the report consists of a general description of vendor responsibilities. It should contain the following information.

Vendor – Indicate the vendor's name, corporate address, and the name of a contact person.

Date – Indicate the date the software review began.

Application Software System– Describe the software system being reviewed and include the system description and capacity for hardware, software, and telecommunications. Describe:

- The system software requirements.
- The software's capacity by determining the number of accounts, number of transactions, telecommunication speeds, etc.
- The release level(s) of the software product supported by the vendor.
- Hardware requirements to operate the software (include disk and memory requirements).
- The capacity of the storage devices.
- The telecommunications network that includes the applications, hardware, and compatible devices required to operate it.

Type and Number of Users – Indicate the total number of financial institutions using this software by type of institution.

Organizational Structure – Describe briefly the corporate and financial history of the vendor.

User Group Contact – Indicate the user group liaison.

EXAMINER'S CONCLUSIONS

Briefly summarize the significant findings of the report sections, in the following order: Audit, Management, Systems Development and Programming, Operations, and Networking.

INTERNAL/EXTERNAL AUDIT

Audit Software – Determine if the institution uses the audit software included with the software package or another audit program. If another program is used, determine why. Describe audit software if it is included with the software package. Review the documentation provided.

External/Internal Audit – Determine whether the software has been reviewed by internal or external auditors. Note any deficiencies disclosed and determine the necessary follow-up.

MANAGEMENT

Management Staff/Succession – Determine whether the vendor has sufficient staff to maintain the software. Address the depth of staff and provide for adequate management succession.

Training – Comment on the extent of vendor provided training.

User Groups – Ascertain if there are user groups that meet regularly to discuss software deficiencies, future plans, and current topics. Comment on the vendor's responsiveness to the user groups' concerns.

Source Code – Determine whether the vendor provides a source code and program/system documentation or, if not, whether an escrow agreement exists. The related code and documentation should be under the custodianship of a disinterested third party. Determine if the code and

documentation are subject to audit and if the frequency of these audits is appropriate.

Costs/Fees – Decide whether vendor costs/fees are reasonable. The examiner should consider upgrade fees, training costs, conversion costs, and other related expenses.

Vendor Support – Determine whether the vendor provides adequate continuous support to meet the needs of the user.

Contact Hotline – Determine whether a technical support contact is available to resolve software problems encountered by the user.

Future Issues – Document the vendor's plans, including future releases and required hardware upgrades.

Accounting Issues – Review vendor provided software accounting guidelines relating to purchase costs and incremental installation/conversion costs and comment on whether they comply with GAAP.

Compliance Methodology – Determine whether the vendor has a regulatory compliance office; how the vendor becomes aware of regulatory changes; and whether the software provides reports that comply with applicable laws and regulations.

Insurance – Provide a description of the vendor's fidelity bond coverage.

Contracts – Review existing contracts between the vendor and user. Determine if the contract conforms with FFIEC guidelines.

SYSTEMS DEVELOPMENT AND PROGRAMMING

Documentation – Determine the quality of the documentation provided and whether it is current. This review should address only vendor provided documentation. However, the examiner should be aware of enhancements created by the user.

Programming Documentation – Determine whether the systems development and programming documentation includes:

- System narrative.
- System flowchart.
- Program narrative.
- Program flowchart.
- Data elements.
- File layouts.
- Descriptions of edits.
- Report layouts.
- Descriptions of tables.
- Current source listings.
- Program change history.
- Other elements considered necessary by the examiner.

Utilities – Identify all data altering utilities. Determine whether the application has its own utilities or relies on operating system utilities. The examiner should identify any other utility programs that affect the control environment and identify applicable controls.

Release Process – Identify the vendor's latest software version and the one at the institution, noting the release and implementation procedures. Indicate the extent to which periodic updates are required, such as year-end updates.

Software Controls – Identify built-in software controls that may include:

- Limit checks.
- Range checks.
- Alpha/numeric checks.
- Reasonableness checks.
- Check digit tests.
- Run-to-run totals.
- Date checks.
- Hash totals.
- Batch totals.
- Tests for zero/blank fields.
- Test for mathematical sign.
- Field and code value checks.
- Edit tests.

System Requirements – Determine the system software requirements and the required resources.

Software Capacity – Analyze the software's capacity by determining the number of accounts, number of transactions, telecommunication speeds, etc.

Audit Trail – Determine whether audit trails are in place to trace and record all transactions. All transactions should be listed on a transaction register and all exception transactions noted on an error/suspense report.

Systems Development Life Cycle (SDLC) – Determine if an SDLC methodology is used by the vendor. Comment on the level of user involvement throughout the SDLC process and the effectiveness of user participation. (See Chapter 9 Systems Development Life Cycle and Waterfall System Development.)

Programming Languages – Describe the programming language used by the vendor to maintain the software. Determine whether it is currently being supported by the vendor. Also comment on the vendor’s ability to maintain

it. Determine if the size and depth of the programming staff is adequate relative to the programming backlog and projects under development.

Software/Hardware Interface – Determine whether the software:

- Interfaces with other software products.
- Is limited to products offered by that vendor.
- From another vendor which has been added, violates the licensing contract.

Program Maintenance – Describe the process for performing program maintenance. Determine the utility programs necessary to install program changes. Determine how new releases are moved into production.

Software Maintenance (Vendor Supplied) – Determine whether the vendor provides program maintenance. If so, determine what procedures are in place to handle these changes and current documentation is provided with each update. Comment on the adequacy of vendor testing.

DATA INTEGRITY

File Maintenance – Identify how file maintenance is performed by answering the following questions: Can the user perform file maintenance on all files and fields within each record? Which fields are locked out? Who is authorized to perform file maintenance? Is knowledge of a programming language required? If so, which ones? Are procedures well documented? What type of security is in place for this process? (See Chapter 14.)

Output Reports – Determine whether the reports meet the user's needs. Are they easy to read and understand? Does each report have a specific heading or title page? Does the software include report writer capabilities?

Input Controls – Identify software input controls. Address controls for error checking, input validation, and supervisory overrides.

Input/Output Balancing – Review the user's manual for instructions and examples on how to reconcile various reports. Additionally, note whether the instructions are concise and clear.

Error Exceptions – Review the vendor provided documentation and determine whether there are error and edit routines for all critical fields. Review the type of error and exception reports that are provided and whether they are adequate. Ensure that the exception report shows a before and after correction and states the problem and how to correct it.

OPERATIONS

Hardware Capacity – Determine the number of accounts that can be processed by the system and the transaction capacity of the software. Determine if the file size and transaction volumes are monitored to ensure that users are aware of hardware/software utilization.

Utilities – Identify utility programs that have the ability to alter or destroy data and program files. Describe the controls in place to monitor usage.

Restart/Recovery – For selected applications, identify the vendor provided restart/recovery procedures. Determine whether the processing can be restarted without returning to the previous days work.

Documentation – Review the quality of operator and user documentation. Note whether the documentation provides clear instructions to the user.

Backup – Identify the procedures necessary to backup program and data files, including master and transaction files.

Logging – Decide whether hardware features provide for an audit trail of system functions through a console log. Describe logging procedures.

Operating Systems – Decide whether the software vendor provides operating system maintenance.

Contingency Planning – If contingency planning is provided by the vendor, determine the adequacy of the plan, whether it complies with FFIEC policy, and whether it:

- Has been tested periodically, with results reported to the board of directors or designated committee.
- Is comprehensive.
- Addresses telecommunications.
- Provides for all hardware in place at the backup site and is compatible.

Performance – Determine whether there are system characteristics that could impede performance and telecommunications response time.

Maintenance Agreements – Note whether hardware maintenance is included in the software contract, if leased from the vendor.

NETWORKING AND CLIENT/SERVER

Description – Provide a general description of the telecommunication network, including the applications, hardware, and compatible devices required to operate. Identify the devices the system can support.

Data Security – Identify the security system in place to protect the network and related applications. Determine whether it provides the user with the ability to implement levels of security by user or application and provides CRT lockout and time-out capabilities. Verify whether the security package is vendor supplied or an independent package. Describe security reports available.

EXAMINATION AIDS

Description – Determine if a report generator option is available to the users. Provide any information on software capabilities or reports that may facilitate examination efforts of institutions (including IS, safety and soundness, trust, bank holding company, or compliance examinations, or financial institution liquidations) that use this software program. The examiner should list and briefly describe these reports.

Microcomputers – Indicate whether the vendor provides the capability to upload and download information to and from microcomputer files.

ADMINISTRATION SECTION

Description – Prepare a recap of program participants, indicating name, agency, and examiner hours on the job. Also provide any information that may be of assistance when scheduling a subsequent review of this software product, such as contacts.

Future Plans – Discuss the future plans of the vendor.

User List – Provide a list of user institutions using the software product being reviewed.

Turnkey Workprogram – Provide responses to the Systems and Programming (see Chapter 12) and any other applicable section of the FFIEC Community Financial Institution IS Workprogram (see Chapter 23 - Community Financial Institution Examination Program).

OFF-SITE

_____ 1) Send notification letters to the corporate headquarters of the vendor selected for review and the financial institution at which the review is to be conducted.

_____ 2) Perform background research on vendor. Information to be obtained from the vendor to assist the examiner-in-charge should include:
- User list by type of financial institution.
- User group information.
- List of vendor software manuals provided with the software package.
- Copy of standard software contract or licensing agreement.
- Copy of vendor insurance coverage.
- Information pertaining to the vendor's future plans.
- Vendor's latest annual financial statement or annual report.

_____ 3) Prepare an information package for examiners participating in the shared application software review. Materials to be included:
- Name and address of vendor.
- Name and address of financial institution where the review is being conducted.
- Contact person at the financial institution and vendor.
- Location, time and date review is scheduled to begin.
- Vendor profile (include a brief corporate history and organizational structure).

_____ 4) Send information package to examiners scheduled to participate in the review.

ON-SITE

_____ 5) Conduct a brief meeting with data center management, including vendor if on-site, to reiterate the purpose of the review.

_____ 6) Discuss assignments with participating examiners.

_____ 7) Select applications for detailed documentation review.

_____ 8) Make arrangements for an exit meeting with the vendor.

_____ 9) Submit a final written review, along with an electronic version, to the lead agency's Washington, D.C. office for final review and distribution.

SAMPLE INSTITUTION NOTIFICATION LETTER

<Date>

<Name>
<Title>
<Financial Institution>
<Address>
<City, State, Zip>

Dear <Addressee>:

This letter is to inform you that a software review of <software product> is scheduled to take place at your bank commencing <date>. The review is scheduled to take approximately two weeks and will follow the regularly scheduled IS examination of your data center. The <agency name> is in charge of the software review and will be assisted by representatives from the <name participating agencies>. The software vendor has been requested to provide support for this review.

In brief, the Federal Financial Institutions Examination Council has instituted a Shared Application Software Review (SASR) program to review "turnkey" software programs which are widely used by insured depository institutions. This program is designed to assist the federal regulators in developing more consistent examinations of data centers using "turnkey" software and to more efficiently use examiner resources. The review is intended to report the characteristics of the software program such as: operating environment, output reports, audit and control features, upgrade and maintenance procedures, as well as other information to assist examiners in conducting examinations of data centers using this software product. No rating of the software will be assigned nor should this review be construed as an endorsement of this product. The review report is solely for internal use by the FFIEC member agencies. No report copies will be made available to user institutions or to the vendor.

If you have any questions regarding the upcoming review, please contact <name> at <phone number>.

Sincerely,

<Name>
<Title>

SAMPLE VENDOR NOTIFICATION LETTER

<Date>

<Name>
<Title>
<Corporate Name>
<Address>
<City, State, Zip>

Dear <Addressee>:

This letter is to inform you of an upcoming software review of your <software product>, which is scheduled to take place at <financial institution & location> commencing <date>. In 1991 the Federal Financial Institutions Examination Council (FFIEC) instituted the Shared Application Software Review ("SASR") program wherein the federal regulatory agencies comprising the FFIEC would conduct in-depth reviews of widely used "turnkey" software programs. The reviews are designed to assist federal regulatory agencies in developing more consistent examinations of data centers using this product and to more efficiently use examiner resources. It is intended to report the characteristics of the software program, such as operating environment, output reports, audit and control features, upgrade and maintenance procedures, and other information to assist examiners in conducting examinations of data centers using this software product. No rating will be assigned as a result of this review nor should this review be construed as an endorsement of this product. Although the review will culminate in a report, it is solely for internal use by the FFIEC member agencies. No report copies will be made available to your organization or the user financial institutions. An exit meeting will be scheduled at the conclusion of this review to discuss the overall findings and any concerns, if applicable.

You are encouraged to make available a contact person to whom questions can be addressed. To facilitate the review enclosed is a vendor request list which should be completed and returned to my attention by <date>. Thank you for your assistance and prompt response.

If you have any questions, please contact <name> at <phone number>.

Sincerely,

<Name>
<Title>

Enclosure

SHARED APPLICATION SOFTWARE REVIEW VENDOR REQUEST LIST

To facilitate the review process and to minimize the disruption to your organization, kindly assist us by:

- Providing copies of the latest audit of the company or third-party reviews of the software.
- Describing briefly the corporate and financial history of your firm and providing an organizational chart.
- Listing the companies licensed to sell the <name> software package, including a copy of the franchise or licensing agreement.
- Describing briefly the programming staff supporting the <product name>.
- Describing future software enhancements and planned future releases for the <product name>.
- Describing how your company monitors regulatory changes to ensure that your software product complies with applicable laws and regulations.
- Describing insurance coverage, including fidelity bond and errors and omissions insurance.
- Providing copies of your firm's last three annual reports. If your company does not prepare an annual report, please provide copies of the last three fiscal year-end financial statements and statements of income and expense. Also, include quarterly information to date.
- Providing an overview of the <software> system, as well as the applications it supports.
- Listing the various programming languages used.
- Identifying the release levels of the software that you currently support.
- Providing an overview of the System Development Life Cycle ("SDLC") methodology used by your company. Also, describe what user involvement is employed within your SDLC program.
- Describing the process for performing program maintenance and list the steps the institution would find necessary to install the program changes.
- Describing release information and other maintenance documentation provided the institution as part of the release process.
- Describing software capacity information related to number of accounts, number of transactions and number of institutions that the software will support.
- If the source code is maintained in an escrow agreement, providing..
  - The name and address of the escrow agent.
  - A listing of materials stored with the escrow agent.
  - A description of procedures to ensure that the most current copy of the source code is at the escrow location.
  - A copy of the most recent audit of the escrow storage.
  - A copy of the escrow agreement.

- A copy of the authorized user list provided to the escrow agent.

- Describing the hardware requirements to operate the software, including disk and memory requirements.
- Detailing the hardware features for logging system activity and whether a facility exists to specifically isolate the usage of sensitive transactions and utilities.
- Listing any software characteristics or conditions which could impede system performance and telecommunications response time.
- Providing a general description of the telecommunications network which includes applications, hardware, and compatible devices to operate. Additionally, list the number of terminals that this system can support.
- Identifying the security system in place to protect the network and related applications. Also, describe the levels of security that the user may implement.
- Providing a customer listing of institutions using the software. The list should include total number of institutions by type (i.e. national, state member, state nonmember, savings and loan, and credit union).
- Describing briefly the initial and continuing education programs offered financial institutions.
- If user groups are maintained, noting how often they meet. Also, describe future plans, product enhancements, and current issues that have been generated by the user group.
- Providing a copy of a blank standard contract/licensing agreement. Indicate standard contract period and renewal options.
- Providing a copy of software accounting guidelines for purchase and incremental installation/conversion costs are provided to your customers.
- Listing other products or services are offered to financial institutions.
- Providing a list of standard and custom reports available to the bank.
- Describing any personal computer activities supported by the software product.
- Describing any report writer packages that are compatible with or supported by this product.

SAMPLE ACKNOWLEDGMENT LETTER

<Date>

<Name>
<Title>
<Corporate Name>
<Address>
<City, State, Zip>

Dear <Addressee>:

This letter is to acknowledge your company's assistance at our review of your firm's <software product> which began <date>. The review was performed by representatives of this office, the <participating agencies> at the <financial institution>. Your staff was most helpful in our efforts to review your <software product> banking system.

The software review program is designed to assess software products at one location to reduce subsequent reviews at other institutions. The final report will assist regulatory examiners in their examinations of financial institutions that use the <software product> software package.

This review will not result in the assignment of a rating. The resulting report from this review is confidential and for the internal use of the participating FFIEC member agencies. Copies of the software review will not be distributed to participating vendors or user institutions. Additionally, vendors are not permitted to disclose the fact that their software products have been reviewed by the FFIEC.

Again, your assistance in this program is appreciated.

Sincerely,

<Name>
<Title>

SAMPLE COVER PAGE

SHARED APPLICATION SOFTWARE REVIEW

_____
Software Product Reviewed

_____
Software Vendor

_____
Vendor Address

_____
Date of Review

_____
Lead Agency

PARTICIPATING AGENCIES

THIS REPORT IS STRICTLY CONFIDENTIAL
THIS REVIEW IS THE PROPERTY OF THE FFIEC MEMBER AGENCIES AND IS NOT TO BE DUPLICATED WITHOUT PERMISSION. THIS REVIEW IS FOR INTERNAL USE ONLY.

SAMPLE TABLE OF CONTENTS

A table of contents should be provided immediately following the report cover.

Table of Contents

General Overview .....
Examiner's Conclusions.....
Internal/External Audit.....
Management .....
Systems Development and Programming.....
Data Integrity .....
Operations .....
Networking.....
Examination Aids .....

INTERNAL/EXTERNAL AUDITS CHAPTER 8

(FILE NAME ON DISK # 1 = S1C8.WPD)

The FFIEC member agencies believe that a strong internal auditing function combined with a well-planned external auditing program substantially increase the probability that an institution will detect potentially serious technology-related problems. A strong internal auditing function helps to assure a proper control environment and promotes accuracy and efficiency in an institution's operations. An external auditing program complements this function by providing an objective outside view of the institution's bank's operations.

Adequate internal controls should be structured to assure senior management that:

- Records are being processed accurately and in a safe and sound manner.
- Accounting data is reliable.
- Operating procedures are efficient and effective.
- Procedures are in effect to assure continuity of services.
- High risk conditions, functions, and activities are identified and effectively monitored.
- There is proper adherence to management standards and policies, applicable laws and regulations, regulatory statements of policy, and other guidelines.

An independent audit must be performed to ensure that these controls are maintained effectively.

The institution's board of directors must provide for an adequate independent audit. This audit may be performed by the board of directors or one of its committees or it may be delegated to other qualified persons. The board may either:

- Provide an internal audit function capable of evaluating information systems controls.
- Engage outside consultants or auditors to perform the audit.
- Use a combination of both methods to ensure that the information systems area has received adequate audit coverage.

Regardless of the method used, the auditor should report and be accountable to the board of directors or its designated committee. This accountability precludes the auditor from certain relationships that may compromise audit independence.

This section provides a general discussion of the information systems audit function and objectives and methods that may be used to provide appropriate audit coverage. Since information systems is an ever-changing field, this section should be used as a guide in understanding the purpose of a sound information systems audit program, regardless of how technological innovations affect its operations.

EXTERNAL AUDIT POLICY GUIDANCE

Financial institutions of all sizes are encouraged to have both internal and external audit coverage of IS activities. All financial institutions should develop and maintain an appropriate level of external auditing activities. The Federal Deposit Insurance Corporation issued two policy statements primarily targeting smaller community banks in 1988 and 1990 respectively. They covered in some detail guidance addressing both independent external auditing programs and external auditing procedures. These two policy statements, dated December 28, 1988, and January 22, 1990, can be referenced in their entirety in the Chapter 26 of this Handbook. The 1988 policy acts as an appropriate reference for all banks. It specifically encourages state nonmember banks to adopt an external auditing program that includes an annual audit of financial statements by an independent public accountant. The 1990 policy statement provides external audit procedures to be included in a comprehensive external audit program. These guidelines also include basic audit procedures for IS activities.

SELECTING THE AUDIT STRUCTURE

The institution should have written guidelines for the conduct of the information systems audit. The selection of auditor(s) should be approved by the board of directors.

Although the board may delegate the audit performance, it must ensure their quality. The board must periodically review and approve:

- The qualifications and independence of the audit function.
- The scope and frequency of the audit, based on an assessment of risk.
- The current year's audit schedule.
- Reports comparing actual audit work performed versus the approved audit schedule.
- The techniques used in performing the audit.
- The overall condition of the organization's information systems controls and operations.
- Management's actions to resolve material weaknesses cited in audit reports.

Information systems audit coverage may be provided by an internal audit staff, external auditors, or a combination of both. Audit personnel must have sufficient information systems expertise to perform data processing audits. This expertise should be commensurate with the scope and sophistication of the institution's data processing environment. If the internal expertise is inadequate, external sources, such as management consultants, CPA firms, qualified professionals or correspondent banks should be contacted to supplement or perform, the information systems audit function.

Financial institutions increasingly receive outside information systems services from wholly owned subsidiaries, affiliates, bank service corporations, facilities management groups, or independent service companies. The contractual agreement between the service provider and the institution must define audit responsibilities. The board of directors should determine the type of audit that is best for the institution and consider various approaches that include:

- *Audits by the servicer's internal auditor*. To rely on this approach, the board of directors must be assured of the independence, competency, and scope of the audit and it must evaluate the audit results. All exceptions noted in the audit should receive follow-up review to ensure proper resolution. Integration of the serviced institution's internal audit program with that of the servicer should be considered.
- *Audits by an institution's internal or external auditor*. Audits completed by the internal or external auditors should be complimentary in scope and quality. They will be linked directly to its information systems control features or be part of its overall audit. Audit personnel should possess sufficient information systems expertise to conduct an effective audit.
- *Audits through a third-party review*. This method provides for a qualified auditor, who is independent of both the servicer and the serviced institution(s), to review the servicer's operation. The scope of the review is determined normally by the third-party auditor and should be detailed enough to satisfy the audit objectives of the serviced institution and servicer. Generally, the review would complement the financial institution's internal audit program. (Further discussion of third-party reviews may be found in later in this chapter.)
- *Cooperative audits*. If many financial institutions receive services from a common servicer, they may arrange for one audit that would satisfy the requirements of all the participating serviced institutions, i.e., user group. These audits may be performed by internal or external audit personnel. This method should incorporate the following guidelines:
- All serviced financial institutions should be invited to participate in the audit arrangements.
- Costs of the audit should be allocated fairly among all participants.
- All participating auditors should be qualified.
- The audit should be supervised by a committee of officers or directors representing the participating institutions.
- The audit scope and procedures should be identified and agreed to by all participants.
- The auditors' written charter should identify clearly reporting responsibilities, report distribution, and follow-up guidelines.

Whatever method is used, documentation of the scope and audit findings should be maintained at the serviced

institution. Any follow-up review or review by the board or senior management, together with remedial action initiated to correct disclosed deficiencies, should be similarly documented and kept on file.

ROLE OF THE INTERNAL AUDITOR

The internal audit includes an independent appraisal of information systems operations for the board of directors. Auditors evaluate the day-to-day information systems controls to ascertain whether transactions are recorded and processed in compliance with acceptable accounting methods and standards set forth by the board of directors and senior management. Auditors also perform operational audits, including information systems development auditing, to assure management that policies and procedures are effective as designed and followed by employees. (Refer to Figure 8.1.)

Auditors should furnish management with analyses, appraisals, recommendations, and other comments on activities reviewed. These comments will assist management in using its resources more effectively. The internal auditor is concerned with all phases of business activity and must look beyond accounting and financial records to obtain a full understanding of the operations under review.

The internal auditor should:

- Review, appraise, and report on the soundness,adequacy and application of accounting, financial and other operating controls.
- Promote effective control at a reasonable cost (for example, by suggesting certain controls and stressing their importance).
- Determine the extent of compliance with established policies, plans, procedures, and laws.
- Determine the extent to that assets are accounted for and safeguarded from loss.
- Assess the reliability of and the timely processing of management data developed within the organization.
- Track progress in complying with regulatory requirements and recommendations.
- Recommend alternatives to correct control deficiencies.

Figure 8.1
The Focus of the Audit May Shift

With Permission M. Zola Rapid Systems Solutions, Inc.

The institution's board of directors should adopt a charter or issue a policy statement clearly establishing the responsibilities of internal auditors.

The charter should identify the purpose, responsibilities, and authority of the audit department. It should state clearly the auditor's right to access all records, policies, plans, procedures, and properties and to question personnel about the matters under review. The audit charter should include a statement of audit independence and support from the board of directors.

INDEPENDENCE AND STAFFING OF INTERNAL IS AUDIT

Competence

The overall competence level required for an internal information systems audit function depends upon the size and complexity of its operations and the responsibly delegated to the auditor. In some institutions, the internal audit is performed by a person or group that has no other responsibilities except information systems auditing. In other cases, particularly in smaller institutions, audit responsibility is assigned to an officer or employee designated as a part-time auditor. Such an auditor may plan and perform all audits personally or may use staff

borrowed from other departments. An information systems auditor on a small staff should be a skilled generalist. Always, the information systems auditor should possess expertise commensurate with the sophistication of the system(s) audited.

An internal information systems auditor should have:

- A sound knowledge of bank accounting practices and recordkeeping requirements.
- A firm understanding of management concepts and practices and the fundamental principles of internal control.
- The ability to direct, plan, schedule, and supervise specific audit functions.
- The ability to investigate thoroughly and to document this work.
- The ability to communicate tactfully (orally and in writing) with those subject to the audit and to senior management.
- The ability to derive, summarize, and report criticisms effectively and constructively.
- A general understanding of systems design and project management concepts.
- A general knowledge of operating systems, automated applications, methods of storing and retrieving data files, i.e., programming, file organization and documentation, direct access storage devices, and controls customarily used in information systems.
- Knowledge of, and expertise in, information systems auditing concepts and techniques.
- The ability to identify general installation security measures and work flow, including risk analysis and threat assessment.
- A working knowledge of data processing technology.

A financial institution's hiring and training practices are important in considering the qualifications of information systems auditors. The auditor's education and experience should be consistent with job responsibilities. Although information systems auditors do not have to be computer experts, they should be able to recognize how use of a computer can enhance the audit. As the information system becomes more sophisticated or as more complex technologies evolve, the auditor must be given additional training. In the interim, outside technical experts or consultants could be engaged to assist with more complex audits.

Since the computer environment is evolving as new technologies are introduced, audit management should provide a program of continuing education for auditors. Available sources of technical and information systems audit training include:

- Participation in conferences and seminars sponsored by banking and professional associations.
- Courses sponsored by hardware or software vendors (audit and application), colleges, universities, and local technical schools.
- Self-study and programmed learning (technical periodicals, video instructional programs, etc.).
- Monitored on-the-job training, including in-house cross training.

In institutions where the information systems auditor reports to an audit manager, the manager should be familiar with pertinent technical concepts. This will enable him/her to guide information systems audit work, establish an overall plan for audit coverage, and schedule and coordinate this plan with the general internal audit program. The manager should also coordinate the internal audit department activities with those of regulatory authorities and external auditors.

The overall measure of an auditor's competence is based upon the quality of the work, the ability to communicate work results, and effectiveness in obtaining correction of cited deficiencies.

Independence

The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Generally, the location of the auditor administratively within the organization, the reporting

authority for audit results, and the auditor's responsibilities indicate the degree of their independence.

Internal auditors should be functionally directed by the board of directors or the audit committee. The board must ensure that the audit department does not participate in activities that may compromise its independence. These activities may include preparing records, developing procedures, or performing other operational duties normally reviewed by auditors.

However, auditors should make recommendations to management about procedures that affect information systems controls. In this regard, the audit department should review the control aspects of any new application throughout its development. This should ensure that proper controls and audit trails are included in the application so that an effective audit review can be performed more easily.

The auditor's independence is also determined by analyzing his/her reporting process, findings, and recommendations. For an effective program, the auditor should be given the authority: (1) to obtain all records necessary to conduct the audit, and (2) to require management to respond formally to adverse audit findings and to take appropriate corrective action.

By reporting audit results directly to the board of directors, the auditor assists it in fulfilling its audit responsibilities. Internal auditors should be able to discuss their findings and recommendations periodically with directors who are not officers of the institution. If officers or inside directors attend those meetings, their participation should be limited to encourage candid discussion.

To ensure the auditor's continued independence, the auditors should be informed of the standards they are required to meet in their behavior and work.

INTERNAL AUDIT RISK METHODOLOGY

A proper level of audit coverage of the information systems environment requires an effective audit risk analysis methodology. This analytical methodology should provide the internal auditor and the board with objective information to prioritize the allocation of audit (internal and/or external) resources properly. This should ensure:

- More timely audit reporting on high risk conditions in operating units.
- Enterprise-wide risk control functions (e.g., contingency planning, and corporate information security).
- Project activities related to procurement and implementation of new systems.

At a minimum, the IS audit program should provide:

- Identification of audit units, including systems development projects and enterprise-wide risk control functions, based on understandings of IS risk exposures (e.g., that threaten data integrity, financial condition, financial performance, continuity of operations, regulatory compliance, and customer service).

- Maintenance of the universe of audit responsibility including areas to be audited.

- Maintenance of IS risk-based audit coverage plan (e.g., differentiates high, medium, and low risk audits) that includes explanation of audit frequency and resource requirements.

- Detailed analysis and support for a risk-based annual audit schedule approved by the board of directors.

The auditor must work closely with management and the board to obtain proper understandings and perspective on the information risk exposures.

Frequently, integrated audits (i.e., coordination of financial audits and IS audits) address traditional financial audit test objectives, but sometime fall short in operational auditing. For example, a financial audit would generally not cover certain business controls that are normally inspected in an operational audit of the contingency planning process. These business controls include the mission statement for enterprise-wide contingency planning, the charter statement delineating the scope of management responsibilities, contingency plan performance objectives and criteria, and all other operational requirements for the computer center(s), networking/telecommunications, and business resumption recovery.

INTERNAL AUDIT MANUAL

The internal audit manual should define the role of the audit department within the organization and describe the overall audit scope and objectives. The manual often written by the internal audit department should reflect the needs of the institution and the philosophies of the audit committee or auditor. The procedures should establish appropriate guidelines for auditing information systems operations, applications, and user department controls. An internal audit manual is a prerequisite for an effective audit program.

The manual should be reviewed and approved formally by the board of directors. The board must determine whether adherence to its standards and procedures will result in a comprehensive audit. Once approved, the manual will provide the audit department with uniform standards for performance and serve as a valuable training aid for audit personnel. In addition, it will assist the board in evaluating audit work performed and the competence of audit management.

The manual should contain written policies, standards, and procedures for the audit department. These include:

- Administrative and general department personnel policies, including those relating to goals and objectives, hiring, training, performance reviews, and job descriptions.
- Organizational and reporting structure.
- Areas or functions to be audited.
- Audit frequency and scheduling guidelines, including a description of the methodology used for assessing risk in the areas to be audited.
- Detailed procedures for the audit of all significant applications and functions within automated data processing.
- Guidelines for microcomputer audits.
- Guidelines for audit involvement and review of a system's development life cycle.
- Standards for audit workpapers and reports, e.g., content, format, filing and distribution, and report follow-up.
- Standards and procedures for audit software, including its development, purchase, documentation, use, maintenance, and control.

The manual must be modified periodically to reflect appropriate changes in audit procedures caused by a change in scope or by increased sophistication within the audit department, the data center, or end user departments. If those changes affect the audit program significantly, they should be reviewed and approved by the board of directors.

PLANNING, ORGANIZING, AND SUPERVISING AN IS AUDIT

Planning

The effectiveness of any internal audit program depends upon the soundness of audit practices and proper planning. The more precisely the audit objectives are identified, the more likely supporting procedures will be appropriate and carried out effectively. The planning function includes:

- Setting objectives, formulating procedures, and preparing a budget.
- Obtaining sufficient resources for accomplishing the organization's audit objectives.
- Compiling a list of reports, information, and other aids to be requested from the audited area.
- Assigning responsibilities to accomplish the objectives within budget restrictions.
- Reappraising objectives, procedures, and budgets to meet changing conditions.

For example, the objectives of the information systems applications audit can be accomplished by dividing the task into basic steps. Each step should have a defined purpose and carefully detailed procedures for its completion. Those procedures should give the auditor sufficient guidance to perform the audit yet allow for discretion. As each audit step is performed, the auditor should be able to identify areas that require more extensive coverage.

Organizing

Once the audit plan is developed, the auditor must organize staff and materials to accomplish it. Organization

of the audit plan includes establishing a structure and a system designed to:

- Achieve the objectives.
- Assign responsibilities for carrying out the plan.
- Maintain continuity of organization and responsibility.
- Reappraise the structure and system periodically to ensure their continued effectiveness.

Supervising

Supervision is directing, coordinating, and regulating the audit pursuant to planning requirements and to accomplishing stated objectives. The degree of supervision required depends upon the competence of the persons performing the audit and the sophistication and risk associated with the particular area being audited. Supervision generally includes:

- Determining the scope and frequency of information systems audits.
- Establishing standards, including costs and quality of work, for the audit department.
- Ensuring compliance with audit standards by reviewing and signing off on completed workpapers and audit reports.
- Maintaining the audit standards by monitoring procedures, obtaining feedback, and making appropriate adjustments to meet changing conditions.
- Training personnel to comply with the standards.
- Following-up to ensure that report responses are received promptly and address all points as required under the audit program.

Scope and Frequency of Information Systems Audit Coverage

The scope of the procedures and frequency of internal auditing must be sufficient to accomplish the audit objectives. Covered areas are:

- *Compliance review* – Adherence to established policies, standards, and procedures.
- *Quality review* – The quality of formal policies, standards, and procedures, and of management, efficiency of operations, and the adequacy of procedures and controls.
- *Integrity review* – Fraud detection/deterrence, application program and operating system integrity, application system design and implementation, and monitoring employee activities and access levels.

Within these categories, such functions as reconcilements, data entry control, computer operations, systems development, program change, data communications, output distribution, and user department data processing controls will be reviewed. The frequency of audits should be based on the risk associated with each area of audit interest. Among the factors that auditors should consider in assessing risk are:

- The nature of the specific operation and related assets and liabilities.
- The existence of appropriate policies and internal control standards and procedures.
- The effectiveness of supervision, including policies, operating procedures, and internal controls.
- The potential effect of errors or irregularities associated with the specific operation.
- The sensitivity of the information involved.
- The results of past reviews and the current state of identified problem areas.

All areas of information systems operations should be reviewed within an approved audit cycle or annual review. Audit frequency and scope should be associated directly with the inherent risk in an operation or application function. As such, some activities will be reviewed more frequently than others. The board, or its audit committee, should approve the audit schedule each year. It should be apprised of significant deviations to the audit schedule resulting from budget constraints, staff turnover, or other contingencies. If the audit schedule is not completed within the expected cycle, the reasons should be documented and reported to the audit committee. Major adjustments to the schedule should be approved by the committee or the board.

AUDIT PROCEDURES

Information systems audit procedures will vary depending upon the philosophy and technical expertise of the audit department and the sophistication of the data center and end-user systems. However, to achieve effective coverage, the audit program and expertise must be consistent with the level of data processing activities being reviewed. The audit procedures may include manual testing processes or computer-assisted audit programs. Usually, a combination of manual and computer-assisted audit techniques will be used.

Internal auditors may choose techniques to test records that do not use the computer. For these methods to be effective, the control environment in that data processing is performed must be considered. Such methods may include comparing a representative sample of records with source documents or verifying them independently through direct confirmation. The results of these procedures should be reconciled in the same manner as in an audit of manually prepared records.

When computer audit programs are used, internal information systems auditors should perform application reviews, compliance and substantive tests, and record evaluation, to verify the adequacy of internal controls. Discussions of the implementation of each approach follows:

Application Review

- Use questionnaire.
- Interview personnel in data processing.
- Develop a general system description.
- Review major controls of user and data processing departments.
- Review programmed controls for each application essential to the audit.

Compliance Tests

- Examine evidence relating to controls, e.g., error listings, batch control records.
- Use printouts to trace items in output to source documents, source documents to reports, report totals to controls, etc.
- Check sample transactions for correct processing.
- Assess the adequacy of test data to determine that testing is comprehensive.
- Test accuracy of summary accounts (foot, crossfoot, etc).

- Test samples of detail items by confirmations, reasonableness tests, etc.

Records Evaluation

- Reconcile user control totals to processing activity and computer report totals to general ledger figures.
- Determine that user department, data processing department, and programmed controls function are documented.

Using Computer-Assisted Audit Techniques

Auditors should strive to use the computer in performing audits. The computer can improve audit coverage by reducing the cost of testing and sampling procedures that otherwise would be performed manually. It also can better check data integrity by testing the logical processing of data "through" the system rather than relying only on validations of input and output controls.

Audit software is available to:

- Test footings and computations to verify the accuracy of information systems outputs.
- Test records for completeness, logical consistency, validity of conditions, and reasonableness of amounts.
- Summarize and analyze operating efficiency from job accounting data.
- Test input and output data and controls for authorized processing.
- Select and print data by using statistical sampling techniques for confirmations, etc.
- Simulate independently the processing of transactions to verify the accuracy and consistency of computer programs.
- Generate audit trial balances and related reports.
- Establish an audit software library.

For audit purposes, internal auditors may use:

- Programs written by the internal programming staff or by outside programmers with audit department supervision.
- Generalized audit software, e.g., audit packages offered by CPA firms or software vendors.
- Programs written by information systems auditors.
- Programs available from equipment manufacturers and software houses to analyze machine, programmer, and operations efficiency.

Audit techniques available to test data and programs within the computer systems include:

- *Integrated test facility (ITF)* – Processing test data for a dummy department, branch or function, and comparing processing results to those predetermined. Transactions initiated by the auditor are indistinguishable from live ones and are processed at the same time as live data. Special care must be taken to partition test accounts and balances strictly to avoid understating or overstating assets. The auditor should also be aware of any local legal restrictions to the use of ITFs.
- *Parallel simulation (independent audit proof)* – Using independent software to simulate actual application processing and comparing these results with those of actual processing.
- *Audit logging* – Maintaining a computerized record of all access to a given file, including the accessing terminal and user identification.
- *Parallel operations* – Verifying the accuracy of new or revised application programs by processing production data and files, using both existing and newly developed programs. Processing results are compared to identify unexpected differences. (This technique is employed customarily by programmers and systems' analysts prior to releasing newly developed or modified applications. However, information systems auditors should be involved to ensure the thoroughness of parallel testing.)
- *Base case system evaluation* – Executing computer application programs by using test data sets developed as part of a comprehensive testing program, and verifying processing accuracy by comparing processing results with predetermined test data results. (Such testing should be performed whenever applications are modified.)

- *Embedded audit data collection* – Using audit subroutines embedded within computer applications software to screen and select for audit review input transactions and those generated within applications.

- *Transaction tagging* – Auditing an application by tagging a special code to input records as they enter a given system. The status of the live records is monitored as they flow through specific points in the application.

- *Extended records* – Adding a control field to a given record either as a special field or as a trailer record. This field or record may include data from all application programs that contributed to the processing of a transaction.

Whatever the source, audit software programs should remain under the strict control of the audit department. For this reason, all documentation, test material, source listings, source and object program modules, and all changes to such programs, must be strictly controlled. In installations using advanced software library control systems, audit object programs may be catalogued with password protection. This is acceptable if the auditors retain control over the documentation and the appropriate job control instructions necessary to retrieve and execute the object program from the libraries where it is stored. If internal control procedures within the computer system do not allow for strict audit control, audit programs should not be catalogued. Computer programs intended for audit use should be documented carefully to define their purpose and to assure their continued usefulness and reliability.

When audit software is processed, auditors must ensure the integrity of processing. Appropriate controls include:

- Maintaining physical control over the audit software, unless it is catalogued in the system and protected appropriately.

- Developing independent program controls that monitor or limit the processing of the audit software.

- Maintaining control over software specifications, documentation, and job control language.

- Controlling the integrity of files being processed and output generated.

AUDIT PARTICIPATION IN APPLICATION DEVELOPMENT/TESTING OR ACQUISITION

The development of an automated application may be a lengthy and complex process requiring a significant degree of interaction between the programming staff and user departments. To ensure that applications meet the needs of the institution, the process requires detailed developmental stages, referred to as the system development life cycle (SDLC) or system development methodology (see Chapter 12, Systems Development and Programming). As each stage of the life cycle is reached, the auditor may review internal controls and audit trails included in the application. Modification of a completed application program once in production is usually more difficult and expensive. The auditor should participate in its development to ensure that effective audit controls are incorporated from the beginning. Guidelines should be developed to facilitate the review of new applications during the design phase, so that controls can be identified for early audit review.

Earlier sections of this chapter detail the reasons why an independent objective audit function is necessary. This objectivity need not be compromised by audit input during the developmental cycle of an application. Auditors should be able to determine and recommend appropriate controls to user management. Such recommendations are not intended to be assurances that controls are absolute, but that the structure is appropriate. In this capacity, the auditor is merely a "consultant" on internal controls. Care should be exercised, however, to preclude the auditor from direct involvement in management decisions.

Once a new application system or major revision to an existing system is accepted for production processing, the information systems auditor should schedule a post-implementation review. This should occur within the first year of production. The reviews should provide for more extensive testing and auditing of the program logic, calculations, error conditions, edits, and program controls. Such testing allows for validation that the software controls function as expected. By performing the review soon after conversion to production, processing errors or other unsatisfactory conditions can be identified and resolved. This should minimize potential redesign costs or losses from processing errors or ineffective software controls.

In larger information systems facilities, divisions, such as quality assurance or change management, may have primary responsibility for post-implementation reviews. In such cases, the information systems auditor may choose not to perform a full review, but should participate nonetheless in establishing the test criteria and evaluating results.

AUDIT REPORTS AND DOCUMENTATION

The audit department should establish, within the internal audit manual, standards for audit workpapers and related communications. Workpapers should be well-organized, clearly written, and address all areas included in the audit scope.

They should contain sufficient evidence of the tasks performed and conclusions reached.

Workpaper documentation should include:

- A detailed description of the data center's current operational, administrative, and program controls and procedures.
- A copy of the audit procedures and questionnaire.
- A description of the audit scope, including the extent and results of tests performed.
- Audit supervisor's signature or initials evidencing review and approval.

Formal procedures should exist to ensure that audit findings are summarized and presented to management to communicate effectively the results of the audit. The basic guidelines are to:

- Provide information on scope and objectives.
- Summarize clearly, all significant audit findings, discuss them with line management, and report them in writing to senior management, and the board of directors.
- Discuss with the directors serious control deficiencies uncovered by audit work and any significant audit findings that remain unresolved.
- Highlight succinctly in well-written audit reports exceptions noted, potential risk exposure, and recommendations for remedial action.
- State an overall opinion of the audited function, whether there has been improvement or decline since the function was last audited, and reasons for any changes.
- Documenting in the workpapers all criticisms and observations made in audit reports.
- Have management prepare timely written responses to all audit reports.
- Follow up on exceptions to ensure that corrective action has been taken or that the board of directors has accepted the risk.

Reporting Conclusions

Completion of specific procedures in the information systems audit workprograms should lead internal auditors to conclusions that satisfies corresponding audit objectives. Conclusions must be appropriate for the audit work performed and consistent with documented findings. Auditors must use sound judgment to separate significant and insignificant findings.

Written audit reports communicate audit findings to management. The report should assist management in evaluating the quality of its information systems department and identify and suggest methods for correcting or improving any adverse conditions found. Audit reports should be timely, summarize facts, and indicate the status of previously reported exceptions. Information contained in the reports should be constructive, accurate, and presented clearly and logically, so that any negative audit report finding can more easily trigger a management decision.

Often oral discussions are crucial in presenting audit findings effectively and identifying possible solutions to uncovered problems.

AUDIT FOLLOW-UP

Prompt and effective management response to internal auditors' recommendations should be required in an information systems audit follow-up. The audit procedures should identify clearly the methods for follow-up. These procedures may include:

- Requesting a written management reply to the audit

report that identifies corrective action for each deficiency.

- Subsequent testing of audits to verify resolution of deficiencies.
- Reporting to the board of directors or the audit committee on specific action taken or lack thereof.

When a critical deficiency is noted during an audit, a follow-up review should be performed to ensure that the corrective action has reduced the exposure to an acceptable level. Recommendations not accepted and deficiencies remaining should be documented in the follow-up review and reported to the board.

Without follow-up, even a comprehensive internal audit program will be less effective. Although the desirability of formal procedures is clear, the person or persons responsible for them should take the time necessary to develop effective ones. Often the internal audit manager monitors the progress of audit recommendations. Monitoring techniques must be effective, yet should not antagonize or impair the manager's relationship with operating management.

ROLE OF EXTERNAL AUDITOR

Responsibilities of external auditors should be defined clearly for the board of directors and senior management. This may be done by requiring auditors to submit engagement letters to the board prior to commencing their work. Such letters should discuss the scope of the audit, its length, and resulting reports. Often, essential audit features will be summarized in the letter and schedules attached describing specific procedures for each audited area. The engagement letter may include biographical information on personnel involved and provisions for disclosure and review of audit workpapers by the financial institution, its representatives, or regulatory examiners. In addition, the letter may specify any auditing procedures to be omitted – such as confirmation of loans or deposits – and whether the auditor is expected to render an opinion on the institution's financial statements.

External auditors may review information systems internal control procedures in their overall evaluation of internal accounting controls when auditing the institution's financial statements. CPA standards require auditor/accountants to consider the effects of information systems activity in each significant accounting application.

Generally, external auditors must review the general and application controls that affect the recording and safeguarding of assets and the integrity of the financial statements. General controls include the plan of organization and operation, documentation procedures, access to equipment and data files, and other controls affecting overall information systems operations. Application controls relate to specific information systems tasks and provide reasonable assurance that the recording, processing, and reporting of data are properly performed.

As external auditors review the system of internal accounting control, they should determine the extent that information systems are used in each significant accounting application. That should dictate the extent that information systems controls must be reviewed. The auditor selects the method and specific procedures for evaluating those controls. Most external auditing firms use a questionnaire or work- program to document their review. Generally, these questionnaires cover:

- Equipment, software, and organization.
- User department controls over data processed by information systems departments.
- Program and procedural documentation.
- Processing controls.
- Back up procedures.
- Security.
- Contingency planning.
- Internal audit function.
- Insurance.

External auditors may also make substantive audit tests independent of the institution's information systems operations.

THIRD-PARTY REVIEWS OF SERVICE CENTERS

A service center that processes work for several institutions often is subject to separate audits and

examinations by external auditors, by state and federal agencies, and by internal auditors of the serviced institutions. These audits may be duplicative, creating a hardship on the center management. That burden may be minimized by arranging for a third-party audit to determine the existence and reliability of internal controls at the service center. A third-party audit, in this context, is an audit of an information systems servicer performed by auditors who are not employees of the servicer or of the serviced institutions. The third-party auditor may be engaged by the serviced institutions' management, its auditors, or the service center. The serviced institutions' auditors (internal or external) could use this third-party review to evaluate the system and controls at the service center. Normal regulatory examinations would still be performed.

The objectives, scope, and audit procedures of each third-party audit differ according to the needs of those engaging the auditor. The American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) Number 70 provides guidance for independent auditors when auditing financial statements for an entity that uses a service organization to process its transactions. The statement also guides independent auditors who issue audit reports on service organizations for use by other auditors. Institutions using such audits to complement their own coverage should ensure that the scope satisfies their audit objectives.

Audit coverage of the service center should be as extensive as that which is appropriate for an institution's own computer center. Information systems audits should determine the adequacy of controls in all areas of the data center, including computer operations, systems and programming, and input/output controls. If serviced institutions' auditors are satisfied with the independence, competence, and specific procedures included in the third-party review, they may substitute it for their own audit.

END-USER COMPUTING AUDIT COVERAGE

Financial institution management must provide for an end-user audit function through an outside firm, an internal end-user audit program, or combination of both. The size of the institution's staff is not an acceptable excuse for the failure to meet this responsibility. Smaller institutions can develop and conduct an end-user audit function without significant expense by assigning an officer to create it and by ensuring that it is adequately documented and executed. The independence of the various audit functions must not be compromised by allowing critical portions of the program to be performed by employees who have access to the accounts or the computer. Employees should perform various audit functions in areas distinct from their individual duties and responsibilities. Audit findings should be reported directly to the institution's board of directors or to its audit committee. Independent end-user audit coverage can also be provided by external auditors when conducting their annual review.

All facets of end-user computing should be reviewed within an approved audit cycle. The frequency and scope of the audits should be associated directly with the inherent risk in the operation or application function. As such, some activities will be reviewed more frequently than others. The board of directors, or its audit committee, should approve the end-user audit schedule each year. Responsibility for end-user auditing should be clearly assigned by management. Once performed, the audit procedure and findings should be documented, so they may be reviewed and approved by the institution's board of directors. Completed workpapers provide accountability for the audit function and permit the external auditor and supervisory authorities to review its scope and adequacy.

The scope and frequency of end-user computing audits should be determined by analyzing risks associated with end-user computing networks and other forms of distributed processing. Audit and control procedures should be based on management's understanding of those risks. Procedures and responsibilities to manage these risks should be incorporated into an overall corporate information security policy. In performing an audit of an institution's end-user computing system, an auditor should:

- Check for an adequate end-user computing policy.
- Determine if a department or person has been designated to support end-user computing installations.
- Ensure that adequate policies and procedures are used to evaluate, select, and purchase hardware and software.
- Identify the personnel who have functional responsibilities for control and security.

- Determine the number of PC/LAN's and identify their exact location in the networks and the flow of data between them.
- Review the guidelines and procedures established for auditing end-user operations, information systems applications, and user department controls.
- Verify that PC/LAN terminals are in areas that are physically secure during and after normal business hours.
- Ensure that security policies, procedures, and standards have been written.
- Verify that all PC/LAN terminal usage and transaction processing can be identified with a specific person and workstation.
- Determine if risk assessments for all computer applications and programs have been completed.
- Check for established data backup and recovery procedures and compliance with them.
- Assess the procedures for adequate on-site and off-site storage of backup data and programs.
- Assess the level of user training.
- Determine how access to terminals is controlled.
- Verify data integrity.
- Review controls on using and modifying application software.
- Assess downloading/uploading capabilities.
- Verify that the dedicated file server is in a secured area with limited access.
- Determine that plans exist that reflect how PC/LAN's structure and components will be modified if changes occur in the size of the work group or its geographic location.
- Determine if someone has been identified as the PC/LAN administrator, and whether that person understands his/her responsibilities.
- Verify the access controls to ensure unauthorized access is prevented.
- Identify the person responsible for following up on workstation security violations.
- Review report balancing and employee accounts.
- Check the accuracy of master file information and interest and service charge calculations.
- Perform direct verifications of loan and deposit accounts, mainly by the computer if the application software includes a direct verification program or if audit software is available.
- Review the disaster recovery and contingency plans.
- Verify that the disaster recovery and contingency plans are tested and documented at least annually.
- Verify that confidential data is protected when stored on disk and transmitted on PC/LAN network.

An end-user audit function must be established. The procedures should be expanded and improved as needed.

EXAMINING THE IS AUDIT FUNCTION

Examiners must review management and internal controls of IS departments to determine if adequate information systems audit coverage exists. Periodic comprehensive review is necessary to identify potential control problems and provide independent assurance of the reliability of data processing output. Major factors to be considered in an audit review are:

- Competence and size of the information systems audit staff.
- Independence of the audit function.
- Scope, thoroughness, and frequency of audit coverage.
- Documentation of audit work, including workpapers, audit reports, and follow-up.
- Coordination with external auditors.

The audit staff must be reasonably equipped to perform in-depth audits of all information system related areas, including user controls. The auditor's formal education,

experience, and self-development through continuing education should be reviewed. The auditor's abilities may be discerned further from discussions with them and a review of audit programs, reports, and related workpapers.

It must be confirmed that auditors operate independently of active management and report their findings and recommendations directly to the board of directors or its committee. Auditors must not perform operational functions that may be subject to audit. In addition, the reporting structure should ensure that their objectivity and independence are not compromised by potentially conflicting duties. Audit independence is essential for an effective audit program.

Audit objectives, goals, schedules, and manuals approved by the board of directors should also be reviewed to help assess audit management and the thoroughness of information systems audit procedures. A review of a representative sampling of recent internal and external audit reports should consider the content of the report, its presentation, and whether reports are addressed to appropriate management levels within the organization. Internal information systems audit workpapers should be compared with the appropriate audit procedures to determine that they are being followed. Established follow-up procedures and written responses to selected internal and external audit reports must also be assessed. Follow-up on deficiencies noted in the previous information systems examination must be performed to determine that promised remedial action has been taken.

Deficiencies in the adequacy of the information systems audit staff, independence of the audit function, or completeness of audit coverage must be detailed in the IS Report of Examination (see Chapter 5, IS Examination Ratings and ROE) and communicated to the board of directors.

A review of the audit function should reveal whether any internal or external information systems audit work can be accepted as a partial or complete substitute for regular examination procedures. Acceptance of such recent audit work in lieu of performing some of these same procedures should:

- Reduce the amount of redundancy in the review of information systems functions.
- Ease the burden on data center management and employee time.
- Result in more effective use of examination personnel.

Audits performed by internal or external auditors that meet acceptable standards probably can be substituted for some examination procedures. This cooperation should foster understanding among auditors and regulatory agency personnel and result in better overall coverage.

Information systems audit work must be performed by qualified, independent audit personnel who follow established audit procedures. It should be recent (within the current audit cycle) and germane to existing data processing operations. To justify reliance upon the audit work of others, the audit scope, procedures, and findings should be discussed with the auditor. The audit procedures and workpapers substantiating the adequacy of information systems audit coverage also should be reviewed. Consistent with the scope of the examination if reliance is placed on the information systems audit coverage, the following procedures must be performed:

- Document those work program sections or steps that will not be performed and describe clearly the auditor's findings and conclusions.
- Follow-up on exceptions noted by the auditor.
- Prepare comments for the IS Report of Examination for those exceptions that remain outstanding and significant.
- Note any reliance upon audit procedures in the section of the report describing the scope of the IS examination.

An examiner's detailed review of external audit procedures and workpapers may not always be necessary to comment on the adequacy of information systems audit coverage. However, such reviews may be necessary if external audit coverage is to substitute for any IS examination procedures. If such a review is deemed necessary, the request for appropriate documentation from the outside auditor should be made through the institution under examination. Occasionally, such requests are resisted by external auditors. Under such circumstances, the examiner must use discretion. Section 112 of the Federal Deposit Insurance Corporation Improvement Act

of 1991 (FDICIA) requires that independent public accountants for FDIC-insured institutions provide workpapers and procedures to examiners, if requested.

LEGAL REQUIREMENTS – ANNUAL INDEPENDENT AUDITS

Section 112 of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) added a new section 36 to the Federal Deposit Insurance Act (FDI Act), the purpose of which is to facilitate early identification of problems in financial management through annual independent audits, more stringent reporting requirements, and internal controls. The requirements are contained in Part 363 of the FDIC Rules and Regulations and apply to all FDIC-insured depository institutions with total assets of $500 million or more at the beginning of its fiscal year.

Each covered insured depository institution must prepare annual financial statements in accordance with generally accepted accounting principles (GAAP) that must be audited by an independent public accountant. As of the end of its fiscal year, the institution should prepare a report that contains a statement of management's responsibilities for preparing its annual financial statements and for establishing and maintaining an adequate internal control structure and procedures for financial reporting and for complying with designated laws and regulations. The institution also must include an assessment by management of the effectiveness of the internal control structure and procedures as of the end of the fiscal year and its compliance with such laws and regulations during the fiscal year. Service organizations should be considered in determining if internal controls are adequate. On-site reviews of service organizations may not be necessary to prepare the reports required by Part 363. The institution's independent public accountant, its management, and audit committee should exercise independent judgment in making the determination.

Each covered FDIC – insured depository institution must engage an independent public accountant to audit and report on its annual financial statement. The scope of the audit must be sufficient to permit the accountant to determine and report whether the financial statements are presented fairly and in accordance with GAAP.
The independent public accountant must examine, attest to, and report separately on, the assertions of management about the institution's internal control structure and about procedures for financial reporting. The attestations must be made according to generally accepted standards for attestation engagements.

Part 363 of the FDIC Rules and Regulations, including Appendix A, Guidelines and Interpretations, is contained in Chapter 24, Laws and Regulations.

The objective of this section is to determine whether there is an effective ongoing audit program. These procedures will disclose the adequacy of IS audit coverage and to what extent, if any, the examiner may rely upon the procedures performed by the auditors in determining the scope (limited or expanded) of the IS examination. Document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

BOARD SUPERVISION OF IS AUDIT

1. Review bylaws, board resolution, and audit charter to determine the authority and mission of the IS audit function.

2. Review and summarize the minutes of the board or audit committee for board member attendance and supervision of IS audit activities and determine if the board approves audit plans and schedules, reviews actual performance of plans and schedules, approves major deviations from plans, and reviews audit findings to resolution and the work of external auditors and consultants.

3. Determine if the external auditing program complements the IS internal auditing function/activities.

INDEPENDENCE AND STAFFING OF IS AUDIT

4. Determine that the reporting process for the IS audit is independent in fact and in appearance by reviewing the degree of control persons outside of the audit function have on the board or audit committee.

5. Review the internal audit organization structure for independence and clarity of the reporting process.

6. Determine that the IS audit staff is adequate in number and is technically competent to accomplish its mission.

   a. Review data sheets and evaluate IS audit personnel qualifications to the job descriptions.

b. Determine if staff competency is commensurate with the technology in use at the institution.

c. Review the IS audit budget and discuss with audit management the adequacy of current staffing levels, turnover, and staff training.

OVERALL AUDIT STANDARDS

7. Review the IS audit standards manual and/or IS related sections of the general audit manual. Assess the adequacy of policies, practices, and procedures covering the format and content of reports, distribution of reports, resolution of audit findings, format and contents of workpapers, and security over audit materials.

IS AUDIT PLANNING

8. Determine that the planning and scheduling of IS audit work are adequate to accomplish the mission of IS audit.

   a. Evaluate planning and scheduling criteria (including risk analysis) for selection, scope, and frequency of audits. Determine if:

      1) The audit universe is well defined.

      2) Audit schedules that support the entire audit universe will be reviewed within the audit cycle.

      3) The audit cycle is reasonable as approved by the board of directors .

   b. As applicable, determine the date of the last audit covering:

      1) Management

         a) Corporate Contingency Planning
         b) Management Information Systems (MIS)

      2) Systems Development and Programming.

         a) Programming Controls
         b) Acceptance and Cataloging
         c) Operating System Controls
         d) Data Base Management

e) Reviews of New Applications, Post Implementation Reviews, and Reviews of Existing Application Reviews (List Applications)

3) Operations

a) Physical/Environmental Controls
b) Data Controls
c) User Department Controls (List Departments)

4) Security - Physical and Data

a) Networks/Teleprocessing
b) Data Security
c) Physical Security

5) Networking and Client/Server

6) End User Computing (List Systems)

7) Document Imaging

8) Electronic Funds Transfer (EFT)

a) Wholesale EFT
b) Fedline EFT
c) Retail EFTs (ATM, POS, Debit Card, Home Banking)
d) Automated Clearing House (ACH)

9) Service Provider/Receiver Activities:

a) IS services provided to external users
b) IS services received from external Sources

c) Discuss with audit management significant information systems and data processing activities that have not been audited within scheduled time frames. Areas not audited within scheduled time frames, especially those not completed for an extended period, may be considered for Tier II review.

INDIVIDUAL IS AUDIT PROCEDURES

9. For each area established under IS AUDIT PLANNING (Step 8a. above), determine that the audit procedures employed meet Tier I standards as set forth in the following individual examination steps. Reference is also made to the appropriate chapter and section of this *Handbook* for additional detail supporting Tier I review procedures. Failure to meet these minimum standards may prompt a full or modified Tier II review of the area. Reference below to parts a. through h. Provide an overview of audit coverage across IS areas of activity.

   a. Determine whether audit procedures for **MANAGEMENT** adequately consider:

      1) Personnel policies, including hiring, termination, and training (training should cover awareness training for emergencies, information confidentiality, security, etc,).

      2) Job descriptions and reporting structures are current and appropriate to the job functions and the nature of the organization.

      3) Formal contracts govern activities of contract programmers and other outside consultants and include provisions that subject them to the same policies and procedures as employees.

      4) Insurance issues for consultants have been fully addressed by management.

      5) Adequacy of oversight by senior management, applicable committees, and the board of directors.

      6) Corporate contingency plans are comprehensive, current, and adequately tested.

      7) Management information systems (MIS) provide timely, accurate, consistent, complete, and relevant information.

b. Determine whether audit procedures for **SYSTEMS DEVELOPMENT AND PROGRAMMING** adequately consider:

1) Programming Controls:

a) The institution's formal application development/acquisition methodology and compliance with it.

b) Written programming standards covering coding techniques, documentation, testing, acceptance, and turnover, and compliance with the standards.

c) Segregation of duties between application program development and operating systems programming activities.

d) Program documentation library and/or quality control procedures employed to ensure adherence to systems/programming standards.

e) Controls over on-line programming terminals and access to interactive programming products.

f) Parity of production source and object files (if covered in individual application reviews, note here for cross-reference).

g) Completeness of program documentation, including history of program changes (if covered in individual application reviews, note here for cross-reference).

2) Acceptance and Cataloging Controls:

a) Separation of duties between operations, application programming, and operating systems programming during the cataloging process.

b) Parity between the approved programs and/or program changes to the cataloged version.

c) Approved programs and/or changes are controlled to prevent changes between the approval, testing, and cataloging phases.

d) That test results are properly approved and acceptance authorized before cataloging.

e) That documentation is properly updated.

f) If source code is maintained by the vendor, that an escrow agreement is in effect and the file has been confirmed as being current.

3) Operating System Controls:

a) The controls over utility programs, primarily those with production data or program file altering capabilities.

b) Separation of duties between production data file maintenance and operating system maintenance.

c) Documentation of the operating systems.

d) Controls over system documentation, vendor, and technical engineer manuals, and other sensitive operating system-related materials (access to this information should be limited to those directly responsible for maintaining the system – usually system programmers and/or technical support personnel).

e) Controls over fixes, exit routines, new releases, and other changes to the operating system.

4) Data Base Management:

a) The appointment of a data base administrator.

b) Written procedures employed, including those for maintenance of a data dictionary, and adherence to them.

c) Segregation of duties in maintaining, monitoring, and supervising data base management activities.

d) Effectiveness of transaction logs and procedures to allow recovery of the data base.

e) Data security measures employed to ensure against unauthorized access of data and/or changes to it.

5) Reviews of new applications, post implementation reviews, and review of existing systems to determine that:

a) Systems design is consistent with original objectives.

b) Programs comply with standards.

c) Audit trails and controls are satisfactory.

d) Test plans are/were satisfactory.

e) Test results are satisfactory.

f) Program documentation is adequate.

g) Program changes were reviewed and authorized properly.

h) Program changes were updated properly in documentation.

i) Source and object programs are in parity with each other.

c. Determine whether audit procedures for **OPERATIONS** adequately consider:

1) Physical/Environmental Controls:

a) Computer operations standards and procedures and compliance with them.

b) Reporting mechanisms used by data center management to monitor IS operations.

c) Equipment maintenance and records of equipment problems.

d) Controls over data processing equipment, data files, and production program libraries.

e) Segregation of duties between input, computer operations, and output.

f) Disaster prevention (fire detection, backup power, etc.).

g) Emergency procedures.

h) Housekeeping.

2) Data Controls (If these controls are reviewed by audit as part of other audits, such as computer operations, and user department controls note here for cross-reference.):

a) Evaluation of control points, using flow charts or other techniques (i.e., narratives, matrix).

b) Written procedures and compliance with them.

c) Segregation of duties between origination, input, and output.

d) Control totals generated at input are reconciled at each turnover point.

e) Adherence to formal report processing and distribution procedures.

f) Controls over negotiable and/or sensitive documents generated by the computer.

g) Control over the disposal of printed and magnetic data.

3) User Department Controls:

a) Evaluation of control points, in the user area, using flow charts or other techniques (i.e., narratives, matrix).

b) Separation of duties (input, output, reconciliation, supervision, etc.).

c) Reconcilement of computer records to the general ledger and other control figures (i.e., data entry controls to transactions listing, and hash total used to control non-financial data).

d) Report distribution and usage.

e) Record retention.

d. Determine the adequacy of audit procedures for **SECURITY–- PHYSICAL** and **DATA** for:

1) Data Security:

a) A written data security policy is in effect covering all applications employing teleprocessing systems and compliance with it.

b) Data security activities are independent from systems and programming, computer operations, data input/output, and audit.

c) Access to the systems is restricted by user identification and/or passwords.

d) Access codes are protected properly and changed with reasonable frequency.

e) Transaction files are maintained for all messages entered by terminals.

f) Unauthorized attempts to gain access to the systems are monitored by independent parties.

g) User manuals adequately describe processing requirements.

h) Controls over the telecommunications line used by vendors to maintain software.

2) Physical Security Controls:

a) Access to buildings, computer rooms, and sensitive equipment is controlled adequately.

e. Determine whether audit procedures covering reviews of **NETWORKING-CLIENT/ SERVER**:

1) Written procedures govern the activities of personnel responsible for maintaining the network.

2) The network is fully documented, including remote dial-up, with documentation available to authorized persons only.

3) Logical controls limit access to network software to authorized persons only.

4) Physical controls protect communications equipment, diagnostic equipment, and communications lines from unauthorized access.

5) Adequate network updating and testing procedures are in place.

6) Adequate approvals are required before deployment of remote terminals in homes of personnel and other dial-up locations, and such deployment is consistent with insurance provisions.

7) Alternate network communications procedures are incorporated into the disaster recovery plans.

f. If the institution employs **END-USER COMPUTING**, determine that adequate audit procedures are used to evaluate:

1) The existence of and adherence to a formal institution microcomputer policy.

2) The designation of a function to enforce policies, maintain inventory of hardware and software, and assist users to use the systems.

3) Physical and data security.

4) Data, programming, and security controls on microcomputer applications used for generating official records, making management decisions, and preparing regulatory or management reports.

5) Disaster recovery plans relative to significant microcomputer applications.

6) Software inventory check for use of unlicensed software.

g. If **ELECTRONIC FUNDS TRANSFER** (EFT) activity is performed, determine if audit procedures adequately address:

1) Wholesale EFT.

a) Adequate operating policies and procedures govern all activities, both in the wire transfer department and in the originating department, including authorization and authentication requirements, notification etc.

b) Formal contracts with each wire servicer exist, i.e., FRB, correspondent banks, and others.

c) Separation of duties are sufficient to prevent any one person from initiating, verifying, and executing a transfer of funds.

d) Personnel policies and practices are in effect.

e) Adequate security policies protect wire transfer equipment, software, communications lines, incoming and outgoing payment orders, test keys, etc.

f) Credit policies and appropriate management approvals have been established to cover overdrafts.

g) Activity reporting, monitoring, and reconcilement are conducted daily, or more frequently based upon activity.

h) Activity is covered by appropriate insurance riders.

i) Contingency plans are appropriate for the size and complexity of the wire transfer function.

j) Activity conforms with UCC 4A.

k) Funds transfer terminals are protected by adequate password security.

2) Retail EFT (ATMs, POS, Debit Cards, Home Banking).

a) Written procedures are complete and address each EFTS activity.

b) All EFTS functions are documented appropriately.

c) Physical controls protect plastic cards, PIN information, EFTS equipment, and communication systems.

d) Separation of duties and logical controls protect EFTS related software, customer account, and PIN information.

e) All transactions are properly recorded, including exception items, and constitute an acceptable audit trail for each activity.

f) Reconcilements and proofs are performed daily by persons with no conflicting duties.

g) Contingency planning is adequate.

h) Vendor and customer contracts are in effect and detail the responsibilities of all parties to the agreement.

i) Insurance coverage is adequate.

j) All EFTS activity conforms to applicable provisions of Regulation E.

3) ACH (Automated Clearing House).

a) Policies and procedures govern all ACH activity.

b) Incoming debit and credit totals are verified adequately and items counted prior to posting to customer accounts.

c) Controls over rejects, charge backs, unposted, and other suspense items are adequate.

d) Controls prevent the altering of data between receipt of data and posting to accounts.

e) Controls exist over any origination functions, including separation of data preparation, input, transmission, and reconcilement.

f) Security and control exist over ACH capture and transmission equipment.

g) Clearinghouse and FRB rules and regulations are complied with.

h. Determine whether audit procedures covering reviews of **IS SERVICE PROVIDER/ RECEIVER ACTIVITIES** address:

1) Service provider external users.

a) Formal procedures are in effect and staff is assigned to provide interface with users/customers to control data center related issues (i.e., program change requests, record differences, service quality).

b) Completeness of contracts with all customers (affiliated and nonaffiliated) and that they have been approved by the institution's legal staff.

c) Controls over billing and income collection.

d) Disaster recovery interface between the data center and customers/users.

e) Controls over on-line terminals employed by users/customers.

f) Distribution of comprehensive user manuals.

2) IS services received from external sources.

a) Completeness of contracts and that they have been approved by the institution's legal staff.

b) Satisfactory performance of contracted services.

c) The financial condition of the vendor.

d) Applicable emergency and disaster recovery plans are in effect.

e) Controls over the on-line terminal used by the bank to access files at an external servicer's location.

f) Internal controls for each significant user and/or new application are consistent with those required for in-house systems. (NOTE: Consider the other steps included herein and of third party audit reviews.)

10. If **AUDIT SOFTWARE** is used, obtain a summary listing that includes:

a. Program name.

b. Applications audited with this program.

c. Name of audit software vendor or author (if internally developed).

d. Frequency of use and date last used.

e. SOFTWARE that:

1) Meets the criteria detailed in Chapter 8, Audit.

2) Is appropriate for the size and complexity of the data center.

3) Contains resident programs that are secured adequately in private libraries or otherwise under the control of the auditor.

4) Has related documentation, which is secure and under the control of auditor.

5) Requires the auditor to be adequately trained to make full and effective use of the automated tools.

6) Documentation adheres to written standards for the in-house developed programs and for purchased products. (Note: Documentation standards should be consistent with those developed for the Systems and Programming function.)

Systems Development and Major Program Changes

11. Review the methodology employed to notify the IS auditor of proposed new applications, major changes to existing applications, modifications/additions to the operating system, and other changes to the data processing environment (e.g., equipment configurations, and organizational structure). Determine the adequacy of auditing in:

    a) Participating in the systems development life cycle.

    b) Reviewing major changes to applications or the operating system.

    c) Updating audit procedures, software, and documentation for changes in the systems or environment.

    d) Recommending changes to new proposals or to existing applications and systems.

Audit Reports and Documentation

12. Audit reports

a) If not included in the review of board or audit committee minutes, review reports to senior management that summarize audit activities and findings. Document any unresolved exceptions for follow-up in the applicable section of the workprogram.

b) For each IS audit performed since the last examination, complete the **IS AUDIT REPORT AND WORKPAPER REVIEW SHEET** included in this section and consistent with the scope of the examination determine the degree of examination work to be conducted during this examination (i.e., Tier I only, Tier I with follow-up of audit exceptions, or Tier I and Tier II).

c) Select a sample of workpapers sufficient to determine their consistency in supporting the satisfactory execution of audit procedures and findings. If the workpapers do not generally support audit performance or individual areas, this condition should be considered in determining the scope of review in the other section of the workprogram.

Audit Follow-up

13. Determine whether audit follow-up procedures require:

a) A written management reply addressing each deficiency, including corrective action taken.

b) Subsequent audit tests to verify the resolution of deficiencies.

c) Written reports to the board or audit committee detailing the findings of the follow-up.

External Audit

14. If IS audit coverage is provided by external auditors or outside consultants:

a) Identify the name of the CPA and/or consultant and whether any affiliate or other relationships exist.

b) Review engagement letter(s) and contract(s) to determine the scope and frequency.

c) If external sources are the primary source of audit coverage for all IS activities or specific IS areas, determine that the procedures employed meet the minimum standards set forth in the other applicable steps of this section. Review all reports by completing **IS AUDIT REPORT AND WORKPAPER REVIEW SHEET** and test workpapers to the extent deemed necessary. As applicable determine if the external audits adequately cover:

1) Management/Administration.

   a) Corporate Contingency Planning.

   b) Management Information Systems.

2) Systems and Programming.

   a) Programming Controls.

   b) Acceptance and Cataloging.

   c) Operating System Controls.

   d) Data Base Management.

   e) Application Reviews.

3) Operations.

   a) Physical/Environmental Controls.

   b) Data Controls.

   c) User Department Controls.

4) Security– Physical and Data.

   a) Data Security.

   b) Physical Security.

5) Service Provider/Receiver Activities.

   a) IS Services Provided to External Users.

   b) IS Services Received from External Users.

6) End User Computing.

7) Electronic Funds Transfer.

a) Wholesale EFT.

b) Retail EFTS (ATM, POS, Debit Card, Home Banking)

c) ACH EFT

d. If the engagement was a special review, determine the purpose and whether proper levels of management have reviewed the report. Document the findings in the report and the status of any exceptions noted. All unresolved exceptions should be followed up in the applicable sections of the workprogram.

THIRD-PARTY REVIEWS

15. If significant data processing services are provided by independent data processors, determine whether:

a) Management either employs the services of external auditors directly to evaluate the servicer's controls or requests copies from the servicer of the most recent external audit report.

b) Management requests applicable regulatory agency IS examination reports.

c) All third-party reports are reviewed adequately and followed up appropriately by the auditor.

d) The institution obtains and analyzes the vendor’s financial statements.

CONCLUSIONS

16. Assess the independence, competency, and scope of the internal/external audit function(s) to determine whether audit coverage may be relied upon in determining the scope of the IS examination by:

a) Reviewing IS AUDIT PLANNING (Step 8), INDIVIDUAL IS AUDIT PROCEDURES (Steps 9a through 9*1*) and IS AUDIT REPORT AND WORKPAPER REVIEW SHEETS to determine whether any sections or parts of other sections of the workprogram may require Tier II coverage and/or follow-up for resolution of audit exceptions. Cross-reference with applicable sections to ensure performance.

b) Assessing, audits compliance with Part 363 of the FDIC Rules and Regulations and Statement of Policies 12-28-88 and 1-16-90.

17. Discuss with management:

a) Violations of law, rulings, regulations or significant internal control deficiencies.

b) Recommended corrective action for deficiencies cited.

c) Management's proposed actions for correcting deficiencies.

18. Assign rating. (See Chapter 5 for additional information.)

19. Prepare an index of workpapers for this section of the workprogram.

20. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

21. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

SUMMARY OF EXCEPTIONS

List significant exceptions for follow-up and discussion as determined through the review of audit reports and/or the examination procedures.

Section Name:

IS AUDIT REPORT AND WORK PAPER REVIEW SHEET
(Make additional copies for each audit reviewed.

Name of Institution:
Report Name:
Prior Audit Date:
Audit Date:
Management Response Date:

Date of IS Exam:
Auditor's Name:
Audit Rating:
Report Date:
Follow-up Date:

1. Is the report:

   a. In compliance with the standard format?

   b. Logical, effective, and understandable?

   c. Adequate in describing the scope and objectives?

   d. Adequate in describing significant deficiencies?

   e. Adequate in suggesting corrective measures?

   f. Clear in stating the auditor's opinion/conclusion about the condition and effectiveness of controls in the audited area? Was a rating assigned?

2. Were the objectives reasonable and sufficient?

3. Did management respond:

   a. To the exceptions in a positive manner?

   b. In a timely manner?

   c. With a date of corrective action?

4. Did the auditor:

   a. Review the responses for completeness?

   b. Perform or schedule a follow-up audit?

5. Have the deficiencies been resolved?

6. If workpapers for this area were tested, are they:

   a. Adequate in content to determine that audit procedures have been carried out?

   b. Filed in a uniform manner?

   c. Adequately safeguarded?

Name of Institution:

BIOGRAPHICAL DATA WORKSHEET

PERSONAL

(Name) _____ (Birth Date) _____

(Title) _____

(Responsibilities) _____

_____

_____

(Years with Bank/Center) _____ (Years in Present Position) _____

(Previous Position) _____

(Responsibilities) _____

If employed by bank/center less than two years, provide the following:

(Previous Employer) _____ (Years with that Employer) _____

(Highest Position Attained) _____

(Responsibilities) _____

PROFESSIONAL

(EDUCATION): High School _____ College _____ Bus. College _____
Major Field _____Degree_____
(Indicate number years attended or degree.)

(Continuing Education):

Seminar/Course Title	**Presented by**	**Dates attended**
1. _____	_____	_____
2. _____	_____	_____
3. _____	_____	_____
4. _____	_____	_____
5. _____	_____	_____
6. _____	_____	_____
7. _____	_____	_____
8. _____	_____	_____
9. _____	_____	_____
10. _____	_____	_____

(Membership in Business/Professional Organizations)

1. _____
2. _____
3. _____

Exhibit No. _____
Date_____
Prepared By_____

MANAGEMENT CHAPTER 9

(FILE NAME ON DISK # 1 = S2C9.WPD)

Information processing in financial institutions has experienced rapid change, because of new and enhanced information systems (IS) and technology. These new technologies enable institutions to move data processing resources from centralized mainframe computers to end-user computing systems and distributed processing networks throughout the organization. Third party vendors are also offering a variety of financial products and services to replace or supplement in-house information systems. As a result, a financial institution's IS processing may be performed by a combination of mainframe computer systems, service bureaus, and end-user computing systems. Because of this changing environment, agency and industry emphasis is shifting from the management of data centers to the management of information systems and technology. The FFIEC member agencies recognize this shift from the review of the traditional computer center to that of information systems technology throughout the enterprise. The FFIEC is addressing this shifting focus from a departmental review to an enterprise IS review. The examination approach, scope, and procedures must provide for the effective review of the institution's information systems processing environment.

The management concepts discussed in this section apply to all types of information systems organizations. Data processing services may be provided by a department(s) of the financial institution, a financial institution holding company subsidiary, or an independently owned and operated data center. In this section the term information systems refers to each of these entities.

MANAGEMENT

A review of the management of information systems should determine if it is current and addresses the major technology-related challenges, issues, and problems facing the institution. This includes, but is not limited to, the need for effective procurement and deployment of technology, protection of assets through corporate security and contingency planning, and maintenance of the delivery technology infrastructure through architecture and interfaces. Managing information systems and technology increasingly involves joint cooperative efforts throughout the institution. As a result, the IS examination effort is challenged to study and review an organization's interdependent operations, including the data centers, networks, and user operations.

A review of IS management should determine if it is properly organized, has qualified personnel, and appropriate controls in place. To evaluate whether management is properly organized, reviewers must determine if:

- The management oversight structure is effective (responsibilities may be shared between centralized and decentralized user and outsourced activities).
- The corporate IS policies and standards are well-defined by management and the board of directors. The institution should have an organization chart and policies that specifically define lines of authority and responsibilities for each IS function.

In reviewing IS management, the examiner must determine whether proper and effective supervision and internal controls are implemented and maintained to ensure the integrity of financial reporting and management information systems (MIS). Examiners should also ensure that the MIS meet the decision and reporting needs of the organization. Basic internal control principles, such as segregation of duties, dual custody, and audit trails, are key elements in information systems control. Management also must provide an adequate continuing education program for IS personnel.

ORGANIZATION

The IS function is an inherent part of the financial institution's organizational structure. The function(s) can be centralized in the institution. The senior IS manager should report to the highest level of institution management. An IS steering committee comprised of senior management, is usually formed to provide direction.

The board of directors approves IS plans, policies, and major expenditures, and board members should be familiar with information systems and data center concepts and activities. Senior management must ensure that the board's policies are followed and that the IS function(s) meets the needs of the organization. IS management supervises the day-to-day activities that require a high level of technical proficiency.

Detailed information on organizational structure is essential to review the IS function adequately. The structure and supervision should be evaluated to determine if lines of authority provide for an effective separation of duties.

Organization Charts

The independence of the IS function(s) relative to others can be determined by reviewing the institution's organization chart. Examiners should consider lines of authority and separation of duties. Effective organization charts should graphically illustrate function, the current lines of authority and responsibility. Adequate supervision and segregation of duties should also be evident. Overlapping responsibilities should be questioned, i.e., programmers with computer operator duties or user department managers also in charge of data center operations. Figures 9.1, 9.2, and 9.3 contain sample organization charts. IS organizations have certain characteristics depending upon their size:

- The "small" IS organization chart (Figure 9.1) represents a small holding company or financial institution with an in-house computer. These organizations usually lack an internal programming function. Programming activities are limited, and the software vendor may provide program changes and revisions. An IS management function, such as the one depicted in Figure 9.1, may or may not exist in a smaller institution. Communication tends to be informal and verbal. A complete separation of duties may not be economically feasible. Compensating controls may include cross-training of personnel, dual control over sensitive material, rotation of duties, and independent reviews and audits.

- In "medium-sized" IS organizations with a large number of users (Figure 9.2), the structure is usually more formal. Senior management and the board of directors must be informed of IS activities. End-user computer systems are frequently processing significant applications. This type of organization has a more defined separation of duties than smaller IS ones.

- "Large" IS organizations (Figure 9.3) should have detailed organization charts and position descriptions. They also should have steering committees and regularly scheduled management meetings to enhance communication and monitor activities. Large IS organizations often have multiple data centers and end-user computer systems that operate independently. These independent systems generally are structured as small-sized IS organizations that use microcomputers to process significant applications.

Position Descriptions

Responsibilities should be defined for each data processing function. Usually, they are determined by IS management and tailored to the department's size and complexity. Responsibility, accountability, and reporting authority can be defined through position descriptions. They provide an objective means of measuring job performance when employees understand management’s expectations. Position descriptions and terminology may vary considerably among organizations. The following descriptions provide examples of typical positions that may be found in an IS organization. Not all positions may be present in every organization or several positions may be performed by one person.

Information Systems Manager – Supervises the resources and activities of the IS function, department, or subsidiary; coordinates services between the data processing area and other user departments and reports to senior management on the plans, projects, performance, and matters relating to

information systems.

Operations Manager – Responsible for computer center(s) operation including construction, equipment installation, maintenance, and personnel; Coordinates the daily activities of the computer installation(s); monitors current production to ensure adherence to established schedules. Redirects workflow when processing is interrupted; and provides for cross-training and rotation of personnel.

Operations Shift Supervisor – Coordinates operation of computer equipment during each shift; monitors computer operation and handles most routine problems; may also be responsible for job scheduling.

Figure 9.1
Sample Organization Chart: Small IS Organization

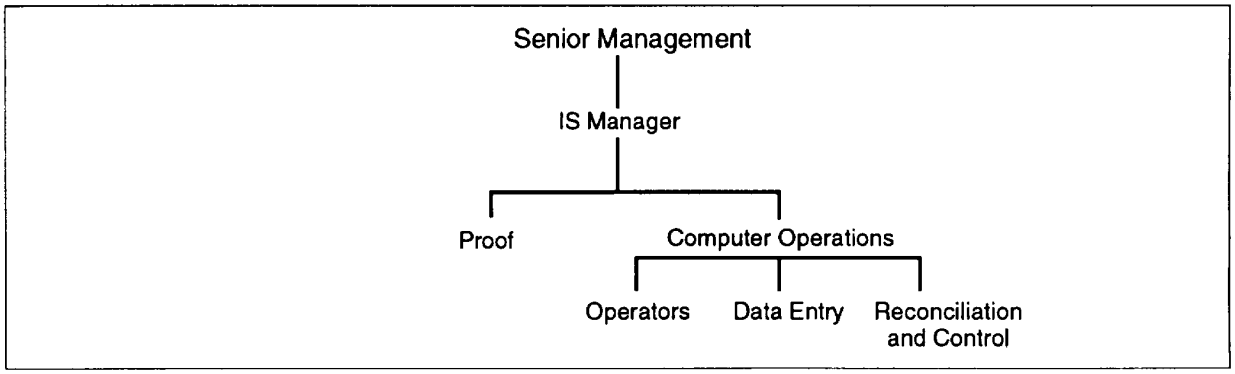


Figure 9.2
Sample Organization Chart: Medium IS Organization

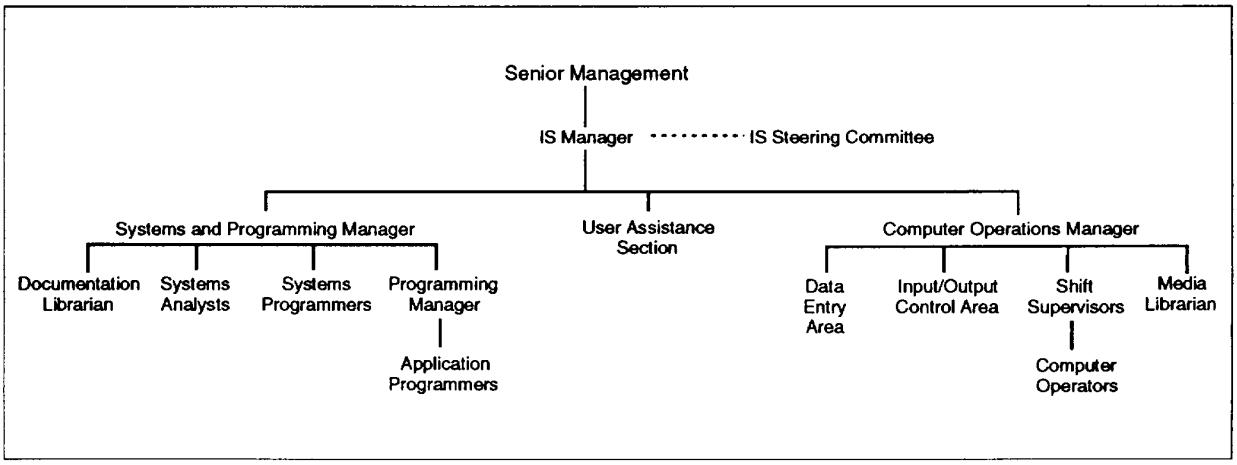
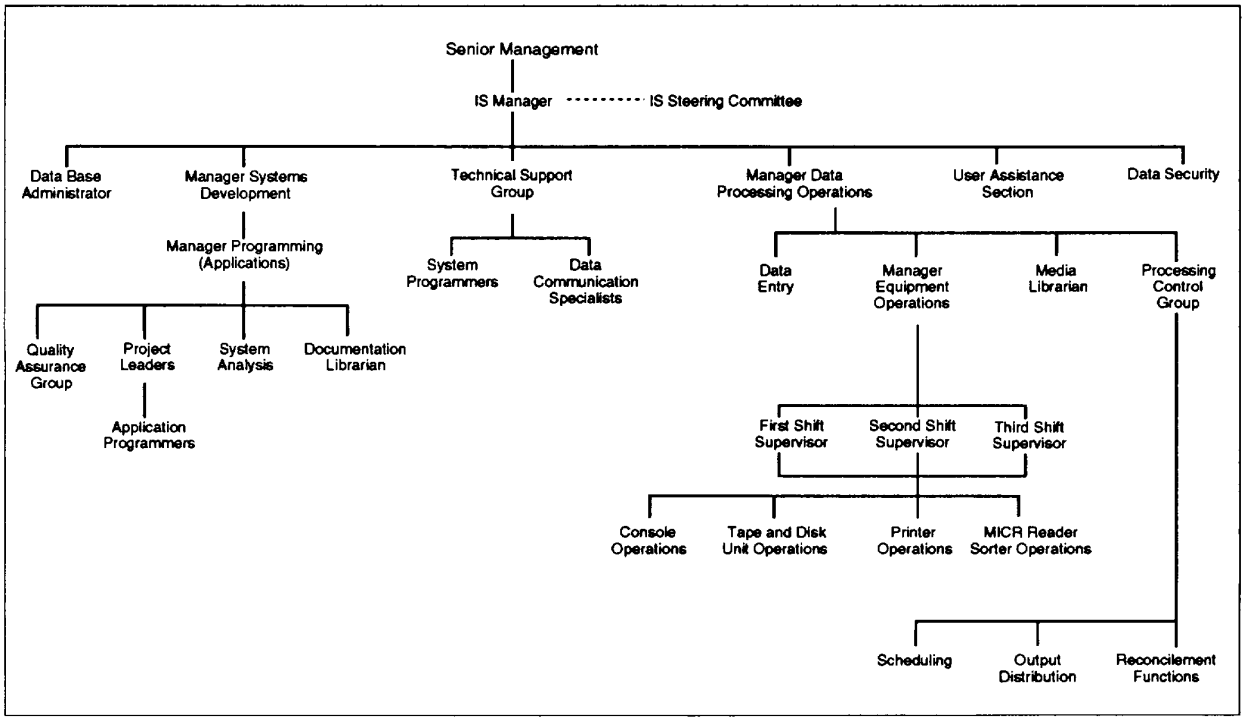


Figure 9.3
Sample Organization Chart: Large IS Organization



Computer Operator – Operates computer hardware according to instructions in Operator's Run manuals. Large installations may have designated operators for computer console, disk and tape drives, and printers. Regardless of the scope of their duties, operators' functions should be limited to those contained in the run manuals for equipment they operate. Operators should not perform any programming or librarian functions and should have access only to documentation necessary to run a given program.

Media Librarian – Has physical control and safekeeping of the center's machine-readable data files and computer programs; also responsibility for accurate disk and tape inventories and for appropriate control and filing of data files. Releases the necessary files for computer production or test runs; maintains accurate records of library activities; ensures that the remote backup library contains appropriate files and is subject to adequate physical control.

Input Preparation Personnel

Proof Operator – Balances and proves the work received from branches, departments, and outside companies; and derives control totals by category for entry into the processing environment.

High Speed Reader/Sorter Operator – Operates equipment which captures the magnetic ink character recognition (MICR) information on documents, converts the information into machine-readable form, and sorts the documents and checks.

Data Entry Operator – Prepares and enters data for processing via terminals or key-to-disk or tape units.

Output Personnel

Reconcilement Staff – Validates accuracy and accountability of transactions; reconciles all output to input control totals; prepares rejected/non-read items for re-entry and makes final reconcilement; and completes user-submitted reconcilement forms to reflect accurate capture or note differences and out-of-balance conditions.

Distribution Staff – Ensures that output is routed and distributed to assigned destinations.

Systems and Programming Personnel

Systems and Programming Manager – Supervises systems and programming staff and coordinates all systems development and programming work for mainframe and PC-based systems; establishes or implements programming and other departmental procedures and is responsible for programming related projects, including measurement of progress relative to predetermined goals and schedules.

Systems Analyst – Analyzes requirements for information processing; evaluates the existing automated systems and designs new or revised procedures for accomplishing the activity; provides the interface between the user of the system and the IS technicians who design it; designs program logic, application system flowcharts, and narratives.

Programmer – Creates and modifies programs and program documentation; converts the program logic into coding suitable for entry into computer equipment; and corrects errors in logic or coding (debugging). The general term "programmer" may be further subdivided into systems programmers and applications programmers:

Systems Programmer – Develops and maintains operating system programs that are necessary for the computer equipment to function, but do not directly perform a production task (such as demand deposit accounting); Usually are responsible for maintaining sophisticated file management routines, data base systems, and large telecommunication networks; Generates, develops, and maintains the operating system; Maintains utilities, job control language, input/output control programs, and control modules; and may develop programs that monitor and measure the performance of the operating system and application programs.

Applications Programmer – Translates instructions from systems analysts to computer requirements and develops, tests, and documents programs that produce the desired actions or products; designs detailed flowcharts, verifies program logic by preparing test data for trial runs, revises and refines programs, and documents all procedures used in finished programs. at a junior level codes, prepares different levels of block diagrams and flowcharts, debugs programs, and assists in various non-critical areas. Has overall responsibility for development, testing, and maintenance of application programs.

Telecommunications Support Manager – Supervises the planning, installation, and testing of telecommunications systems for local and wide-area networks; Directs staff of computer specialists for support of telecommunications resources of organization.

Documentation Librarian – Controls and distributes documentation relating to computer programs; generally reviews documentation of new operating systems and applications to ensure completeness and compliance with standards; and ensures that documentation is updated when modifications are made to existing systems and application programs.

Security Officer – Responsible for the physical and logical security of IS resources and assets; and performs risk analysis to determine the exposures and threats to the computer resources and coordinates with IS and user departments to establish appropriate controls to safeguard resources and assets.

User Assistance Staff – Act as liaison between the computer operation and user departments; provides explanations of output reports generated for user purposes (user reports); and develops technical information, describing input documents and output reports (e.g., user manual).

Technical Support Staff – Act as liaison with computer manufacturer, software support personnel (customer engineers), applications programmers, and systems analysts; and oversees systems development between programming and IS operations; This function usually consists of one or more systems programmers with high technical knowledge.

Network Services Support Staff – Act as liaison with software support and operations personnel to assure a proper and effective on-line communication network. This function is usually staffed with people with data communications and network expertise.

Data Base Administrator – Acts as the clearinghouse and guardian for any requests to change data

representation, deletes data elements (a category of data), or modifies data base access security. This person or group is responsible for the organization of and software security controls over data maintained in a data base file structure.

Quality Assurance Staff – Responsible for reviewing the progress of systems development projects to determine conformity to the installation's standards and procedures. Projects that are substantive in development cost, profit impact, or risk should be reviewed by this group to assure a quality product.

PLANNING

The term "planning" implies preparing for future activities by defining goals and the strategies used to achieve them. Information systems are an integral part of financial institution operations. IS resources must be integrated into the overall management or business planning process. Major investments in IS resources have long-term implications on both the delivery and performance of automated products and services. Independent data centers also must plan effectively, so that they can provide quality and cost-effective service to client financial institutions. Institution management should monitor the strategies and plans of independent data centers that provide services.

Plans may vary significantly depending on the size and structure of the organization. Formal plans should be measured by whether the specific plan being reviewed meets the organization's near term and long range needs. A good plan requires that the board of directors, senior management, and users are involved in the planning process. The board of directors must review and approve the plan. Senior management participates in formulating and implementing it after approval by the board of directors. The individual departments and functional areas, carry out the plan.

Planning can be divided into strategic or long-term planning, and operational or short-term planning, as follows:

- Strategic planning focuses on the long-term use of IS resources to achieve corporate goals. A strategic plan should address long-term goals and outline specific steps and timetables to achieve them. It should include hardware and software architecture, end-user computing resources, and any processing done by outside vendors. The plan should address IS resources for an institution and include a budget(s), periodic reporting of capital expenditures to the board and appropriate committees, and disaster/contingency planning. The final plan should be approved by the board and reviewed periodically to ensure IS performance is consistent with the plan (see Chapter 25, FFIEC issuance SP-7: Interagency Policy on Strategic Information Systems Planning for Financial Institutions).

- Operational planning focuses on short-term actions, e.g., annual planning. The operational plans should flow logically from the strategic plan and be revised at least annually.

An effective planning process may include:

- Developing a mission.
- Evaluating the institution's information systems and technology.
- Assessing the present and future information systems environments.
- Formulating goals.
- Allocating resources.
- Implementing plans.
- Analyzing results.
- Revising the plan.

Financial institutions may differ in the thoroughness and degree of planning. The complexity of operations will determine the formality of the planning process for a particular institution. Plans should always be documented and communicated to the appropriate parties. However, in a small community financial institution, the absence of a written plan does not mean management and the board have neglected planning for the future. For institutions lacking a written plan, the examiner should obtain the information through interviews. Written plans are desirable, but they do not guarantee that an effective

planning process exists. The examiner should evaluate the process as well as the written product.

Critical Factors

The formality and complexity of IS plans, depends on the size of the financial institutions. However, an IS plan should consider the following critical areas in all institutions:

- *Applications software* – Includes changes in software used to provide financial services and products, because of competition, market forces, and changing regulations. These changes may require enhancements to, or replacements of, application software for mainframe and end-user computing systems. Management must anticipate these changes in planning future requirements.

- *Operating software* – Includes operating systems, compilers and utilities that are designed to enable the equipment and applications software to function effectively. Changes in this area can have major impact on hardware and software specifications.

- *Hardware* – Consists of mainframes, minicomputers, microcomputers, communications networks, and peripherals. Planning must ensure that the mainframe and end-user computing equipment has sufficient capacity to meet current needs and future growth. For example, planning may indicate that economically it is impractical to add new mainframe equipment. Rather, it may be appropriate to allow a department to purchase a microcomputer or minicomputer and to operate independently of the main data center.

- *Personnel* – Includes staff changes, scheduling requirements, training, and compensation. Planning should consider whether inadequate salaries could cause high employee turnover or if excessive salaries could suppress earnings.

- *Budget* – Consists of quantifying the financial requirements of the plan. Considerations include, but are not limited to, the potential costs for new applications software, new equipment, and staffing changes.

Information Systems Steering Committee

A management group should oversee the IS planning process. This group may have one of many titles, such as IS Steering Committee, IS Operations Committee, or IS Management Committee. In smaller institutions, the entire board may fill this function. In all cases, a charter defining the role and responsibilities of the committee, and its frequency of meetings, should be developed and ratified by the board of directors. This committee mainly oversees the development and maintenance of the IS strategic plan. It should consist of representatives of senior management, the information systems department, and major end user departments. Internal audit should participate in an advisory, nonvoting capacity.

The committee's duties and responsibilities should be defined in a formal charter. Members do not have to be department heads, but should know IS department policies, practices, and procedures. Each member should have the authority to make decisions within the group for their respective areas.

Such committees typically serve as a general review board for major IS projects and should not become involved in routine operations. They perform the following functions:

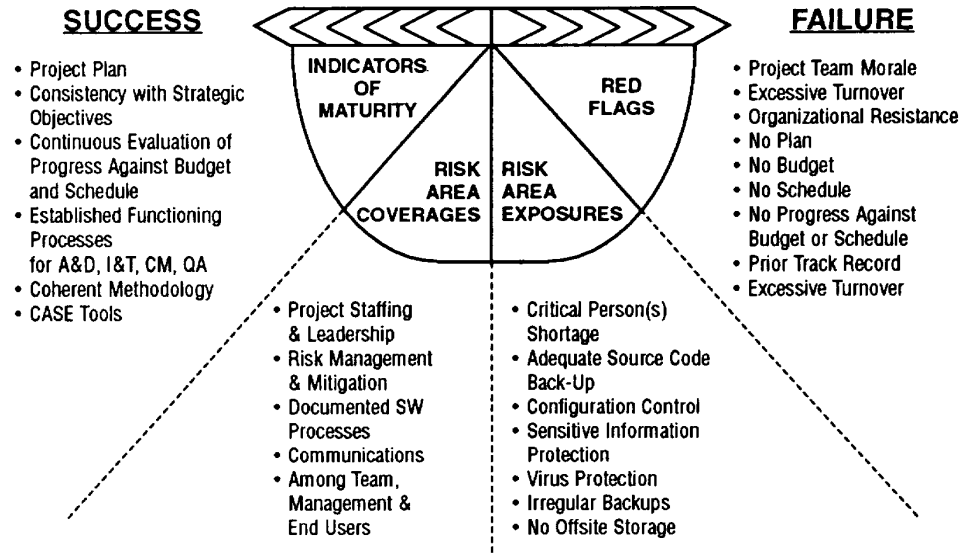
- Review and approve major acquisitions of hardware and software within limits approved by the board of directors.

- Approve and monitor major projects, establish priorities, approve standards and procedures, and monitor overall IS performance.

- Provide liaison between the IS department and user departments.

- Review and approve major IS capital expenditures within board approved limits.
- Approve and monitor major projects, the status of IS plans, and annual budgets.
- Review adequacy of resources and allocation of resources in terms of time, personnel, and equipment.

Figure 9.4
Assessing the Likelihood of Success or Failure



With Permission M. Zola Rapid Systems Solutions, Inc.

The IS steering committee should receive the appropriate management information from IS departments, user departments, and audit to coordinate and monitor the institution's IS resources effectively. The committee should monitor performance and institute appropriate action to achieve desired results. Formal minutes of the IS steering committee meetings should be maintained to document the committee's activities and decisions and inform the board of directors of IS activities.

CONTROLS

The development and implementation of controls within an information systems environment is to ensure the accurate, timely, and complete processing of all work. The control environment encompasses the policies, procedures, and organizational structure of the IS function. The examination evaluates the adequacy and effectiveness of the control environment. The following controls should be considered in this evaluation.

Policies and Procedures

Written policies, procedures, and standards provide the basis for establishing and maintaining proper IS controls. Written standards promote uniform implementation of management policies and aid in training new employees. Management must provide policies and procedures for operating units within the IS department. These policies should provide employees of each unit with the necessary guidelines to coordinate and perform their tasks effectively according to the overall policies and procedures of the organization and the IS department. IS policies and procedures should be developed for:

- The acquisition and use of IS resources.
- Computer operations
- Documentation and standards.
- Data entry preparation.
- Computer utilization.
- Programming activities.
- Output report distribution.
- Information systems security controls.
- End-user computing.

- Insurance.
- Financial analysis of vendors.
- Contingency plans.

Standards and procedures should: (1) allow for separation of duties; (2) limit access to valuable assets, e.g., magnetic media, documentation and computer equipment; (3) ensure authorization of all activity within the data processing area; and, (4) provide efficient and effective allocation of resources. Procedures should provide audit trails to ensure that independent controls are implemented by the user departments.

Internal Controls

Management must establish an effective system of internal controls. Internal controls applied to automated systems are often classified into general and application controls.

General controls are part of the information systems environment and include controls over data center operations, system software acquisition and maintenance, access security, and application systems development and maintenance. They apply to all systems, mainframes, minicomputers, and end-user computing. They include control over modification and maintenance of computer programs, operating systems software, and access to applications and data maintained on computer systems.

Examples of general controls are:

- Management controls.
  - Short and long range planning.
  - Policies, standards, and procedures.
  - Organizational structure.
  - Separation of duties.
  - Personnel training.
  - Internal audit.
- Systems Development and Programming
  - Use of systems development life cycle (SDLC) methodology.
  - Program change procedures.
  - System testing.
  - Access controls and security.
- Data Center Operations.
  - Budgets, hardware acquisition plans, and capacity planning.
  - Physical security.
  - Operating procedures.
  - Backup and recovery procedures.
  - Disaster recovery planning.

Application controls are specific to each application. They are designed to detect and correct errors when entering data into the system and protect the integrity of the application software. Application controls ensure the authority of data origination, accuracy of data input, integrity of processing, and verification and distribution of output. Many application controls use computerized edit checks.

Application controls often depend on general controls. Therefore, the adequacy of the general control environment should be determined before analyzing application controls. For example, a general control procedure may protect against unauthorized changes to computer applications. The adequacy of this general control should be determined before reviewing specific application controls relating to the accuracy and reliability of the data.

Examples of application controls are:

- Data preparation/authorization procedures.
- Document counts/control totals.
- Separation of duties for origination, approval, and data entry of documents.
- File identification checks.
- Application level security.
- Programmed edit checks and reasonableness tests.

If a financial institution uses outside service bureaus for data processing services, their controls should be considered. The institution should obtain and review a copy of the service bureau audit report to ensure that appropriate controls exist to process its data and records.

Management Reporting

Management reporting systems that measure the performance of information systems operating units and the data center(s) is another step in the overall

control process. Reporting may be separated for convenience into different functional areas, such as: (1) operations; (2) systems development and programming; and (3) general/personnel. The types of information, frequency, and sophistication of reports will vary depending on the size and nature of the IS department. Examples of information contained in IS management reports are:

Operations

- Reruns per period by application and total run time.
- Incident or failure reports per period broken down by operator, program, or environment type.
- Telecommunications network downtime.
- On-line failures, terminal response time, and percentage of down time per period.
- Internal label overrides by operator per period.
- Out-of-balance conditions on entry runs resulting in adjustments per period.
- Data entry volume per period by operator.
- Special report runs per period.
- Unauthorized terminal/system access attempts.

Management reports must be reviewed promptly for matters that need management's attention. The review can and should be documented by signing and maintaining copies of reports. For microfiche or microfilm output, management may initiate a review log.

Systems Development and Programming

- Programmer time by project or application.
- Systems analyst time by project or application. (Systems analyst and programmer time may be separated into development and maintenance time. An increasing amount of maintenance on an application may indicate that it is near the end of its useful life. Development time may be compared to projection estimates, and in a sophisticated environment, both methods may be useful in a cost accounting system).
- Status reports on system and programming projects that compare current data to projections.

General/Personnel

- Staffing.
- Overtime hours by functional area.
- Late or missorted deliveries per period.

The board of directors and IS management should determine the quality and quantity of report information needed, and the frequency of reports, in monitoring information systems and data center(s) activities. Senior management and the IS steering committee may require monthly or quarterly data, middle management weekly or monthly data, and first-line supervisors daily and weekly data. Typically, senior management reports include a comparison of prior periods with current performance. Adequate financial reporting systems are necessary for the various levels of management control in an IS installation. These reporting systems generally provide department budgets, budget variance, and internal cost accounting information.

Using the management reporting, management should identify deviations or exceptions from expected performance and make necessary modifications. This may be done by periodic management reviews or independent audits. Management controls to improve performance should address significant areas and be economical, since the cost of establishing and maintaining them should not exceed derived benefits. Although establishing controls is the purview of management, the examiners, auditors, and accountants must specify areas in which they are inadequate.

Independent audits, whether performed by internal or external auditors, measure performance and assess independently the adequacy of policies and procedures. An independent audit program provides management with an impartial evaluation of the information systems department condition. Audit reports should cite exceptions and recommend corrective action. The auditors then must follow up to

ensure that corrective action has been taken. Management must review and follow up on exceptions noted and recommendations made in audit and examination reports.

FINANCIAL ANALYSIS

Independent Servicers

A number of financial institutions contract with independent servicers for information processing services. An independent servicer seeks to generate a profit, rather than break even, as does an IS subsidiary of a financial institution holding company, or operate at cost as does an institution's IS department. The importance of monitoring the financial condition of the servicer cannot be overemphasized. Each serviced institution should obtain and analyze carefully annual (preferably audited) financial statements from the servicer. If the servicers financial condition is weak or deteriorating, the serviced institution should plan alternative arrangements and implement them as necessary. Even if the servicer remains in operation, financial problems often lead to drastic cost-cutting measures that may jeopardize the quality of service and data integrity.

Bankruptcy of a data processing servicer can be devastating to a serviced institution. A 60- to 120-day notification of service termination may not be provided. In this situation, the serviced institution – not the servicer – must find an alternative processing site. Although the user institutions can generally obtain current data files from their servicer, the programs and documentation required to process those files are usually owned by the servicer and may not be available to the users. These programs are often the servicer's only significant assets. Therefore, a creditor, in an attempt to recover outstanding debts, might attach a lien to those assets that limits the availability of these programs and documentation to the users. At this point, the serviced institutions could: (1) pay off the creditor and hire outside specialists to operate the center; or (2) convert data files to another servicer. Either of these options would be costly to the users and could cause unacceptable processing delays.

Data Processing Subsidiary/Department

Generally, an IS subsidiary of a holding company does not affect consolidated earnings performance materially, because it usually provides essential services at costs comparable to or below independent servicers. The subsidiary's financial statement should be analyzed to determine operating expenses. Operating efficiencies may result in lower costs for the center and reduced fees for the serviced institutions. However, this may not always be the case. The contracts between the subsidiary and the member financial institutions it services should be reviewed to ensure that the contracts are "arms-length" transactions that are fair and equitable to all parties.

A financial analysis of an IS department should include a comparison of the cost-effectiveness of the in-house operation versus contracting with an outside servicer. It may also include a peer group comparison of operating costs and ratios with similar sized institutions. Depending upon the size of the institution, costs may or may not be allocated to the user departments. Where cost allocation exists, costs should be commensurate with the services provided to user departments. (See Chapter 25, FFIEC issuance SP-6: Interagency Statement on EDP Service Contracts and OTS issuance TB 46: Contracting for Data Processing Services or Systems).

Budget

A final step in the planning process is the development of an operating budget. Management's plans and its success in meeting budgetary goals are assessed to evaluate data processing management, operations, financial conditions, and prospects. The budget review should furnish insight into the organization's future plans and other matters, such as capital adequacy, liquidity, sources and uses of funds, level and quality of earnings, and management's performance.

The budget is a coordinated financial plan used to estimate and control the organization's activities. By assessing future economic developments and conditions, management creates an action plan and records changes in the balance sheet accounts and profitability (predicated on implementation of the plan). The budget, not only projects expected results, but also serves as an important check on management

decisions and performance by providing a basis for comparison with actual performance. A variance indicated by the comparison may measure management's performance and planning record. Significant variances may be caused by factors beyond management's control or those that could not be anticipated. The comparison of actual performance with the budget allows management to consider alternatives and choose one that should result in the greatest benefit.

Budgeting also measures the performance of persons and the departments they manage. The comparison of budget totals to actual performance promotes coordination and cooperation among affiliates. Although various persons may contribute to the budget process, the chief executive officer typically must prepare and implement the formal budget. The budget often is prepared for one year, although it sometimes covers longer periods in larger, more sophisticated IS organizations. The longer the budget period, the greater are the prospects for increased variances from original budget figures. When four or five projections are made, companies may formulate several forecasts based on different sets of assumptions.

In such instances, the examiner should work with the "most likely" situation that may occur based on economic trends, history, and experience of the organization, but also should consider the "worst case" projections.

Many IS organizations, particularly smaller ones, may not have separate written budgets or plans. Budgeting procedures for IS departments should be encouraged.

INSURANCE

In establishing an insurance program, management should recognize its exposure to loss, the extent to which insurance is available to cover potential losses, and the cost of such insurance. These factors should be weighed to determine how much risk the organization will assume directly. In assessing the extent of that risk, the effect of an uninsured loss must be analyzed, not only on the entity that incurs it, but also on the affiliates and the parent. Once appropriate coverage has been acquired, procedures should be established to review the program periodically to ensure the continued adequacy of the coverage. These procedures should include – at a minimum – an annual program review by the board of directors.

Insurance is intended to complement, not replace, an effective system of controls. Thus, an overall appraisal of the control environment becomes significant in assessing the adequacy of the insurance program. Effective controls and audits may result in lower premiums.

Before insurance is purchased, management should assess the costs of insuring:

- IS equipment and facilities.
- Employee fidelity.
- Media reconstruction.
- Extra expense.
- Business interruption.
- Errors and omissions.
- Loss of items in transit.
- Liability to customers resulting from electronic fund transfer systems (EFTS) activities.

Estimates of these costs will enable management to choose the types and amounts of insurance to carry. They also allow management to determine to what extent the institution should self-insure against certain losses.

Management should review periodically and determine the adequacy of insurance coverage for the computer center and equipment outside of the data processing center. If the computer equipment is leased, it should be resolved who is responsible for insurance – the lessor or lessee. If the lessee assumes that responsibility, insurance must be sufficient to cover equipment replacement or unpaid rentals of the equipment.

An institution or data center can insure against risks covered in various standard insurance policies. However, insurance is generally available for physical disasters,e.g., fire and flood often specifically exclude computer equipment. Those policies usually cover replacement of the physical

magnetic media, but omit the cost of reconstructing the recorded information found in the media. Insurance obtained to provide protection against the hazards inherent in a data processing environment is listed in the following sections.

Information Systems Policy

The IS insurance policy is a multiple peril policy designed to provide various types of coverage. It is constructed so that it can be adapted to the particular institution's IS environment. Specific coverage available and evaluation guidelines are:

- *IS Equipment and Facilities* – Provides coverage of physical damage to the data center and owned automation equipment throughout the institution. Insurance on leased equipment should be obtained when the lessee is responsible for hazard coverage.

- *Media Reconstruction* – Covers damage to IS media, such as magnetic tape and disks, which is the insured's property and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit situations, and covers the actual reproduction cost of the property or, if not replaced or reproduced, the blank value of the media. Considerations in determining the amount of coverage needed are programming costs, physical replacement, and backup expense.

- *Extra Expense* – Covers the extra costs of continuing operations following damage or destruction at the data processing center or other work areas where IS equipment may be located.

- *Business Interruption* – Provides data centers offering outside services reimbursement for monetary losses resulting from suspension of operations, because of physical loss of equipment or media.

- *Valuable Papers and Records* – Covers actual cash value of papers and records (not defined as media) on insured's premises against direct physical loss or damage.

- *Errors and Omissions* – Provides protection against claims arising from negligent acts, errors, or omissions of the insured that occur in performing IS services for others. These policies commonly contain the following exclusions:

  - Employee dishonesty.
  - Libel, slander, or defamation of character.
  - Liability of others assumed by the insured under contract or agreement.
  - Liability of loss or damage to property of others.
  - Personal or bodily injury or sickness.
  - Liability arising out of advice on methods, procedures, practices, etc.
  - Liability for preparation of income tax returns.
  - Loss caused intentionally by, or at the direction of, the insured.

This type of coverage has become increasingly difficult to obtain and premiums (which are normally based on a percentage of outside processing revenues) are often high. In addition, the method insurance companies use to apply the deductible to a claim varies. For example, if a program error caused an overpayment of interest to 1,000 savings accounts, some policies would apply the deductible to each account rather than to the entire overpayment amount. This method would greatly limit the value of the policy to a financial institution. Servicers must review their operations and the benefit of this type of insurance for their specific needs and exposures.

Fidelity

Bankers Blanket Bonds, excess fidelity insurance, and commercial blanket bonds cover loss from dishonest or fraudulent acts by employees. In a financial institution operating its own data processing facility, fidelity coverage is normally provided under Standard Form No. 24, Bankers Blanket Bond. For off-premises processing arrangements (independent data centers, facilities management groups, affiliates or subsidiaries), fidelity coverage has been extended to include the servicer’s personnel as insured under the Bankers Blanket Bond. To qualify for this coverage, the IS services must be provided under a contract between the servicer and the insured. This additional coverage may be deleted by amendment.

In addition to fidelity coverage provided by the user, independent processors often purchase their own fidelity insurance via a commercial blanket bond. An

independent processor operated as a proprietorship may not be able to include the proprietor under this bond. Therefore, serviced financial institutions must obtain coverage themselves.

Media Transportation

One hazard in off-premises data processing is the potential loss of or damage to items in transit between the data center and the serviced financial institution. The standard Bankers Blanket Bond provides limited coverage under specified conditions. In addition, when media is transported via a hired carrier, the insured can apply for an "interpretive letter" from the blanket bond underwriter extending the coverage to the carrier. Normally, the letter will restrict coverage to nonnegotiable property and to the named carrier.

When media is delivered by mail, special data processing transit coverage is available to financial institutions from only a few underwriters. This insurance is designed to cover the transportation of items to and from an IS center, the cost of reconstruction, and the tracing of lost instruments. This policy usually specifies that the insured must make a copy of all documents covered before they are forwarded to the processor. Coverage includes transportation and dishonesty or collusion by delivery employees. Under policies of this type, coverage usually is not limited to nonnegotiables. This is significant since many nonvoided, nonrestrictive, and negotiable items are sent to outside data facilities.

Wording on transit coverage in the policy usually specifies that all documents must be filmed or otherwise copied. When the policy does not specifically state that data be filmed prior to being transported, and it is not, management should obtain from the insurance carrier a letter that describes the carrier's position and coverage in the event data is destroyed.

Electronic Funds Transfer Systems (EFTS)

To limit the risk associated with EFTS, an institution should review available insurance to determine if there is:

- IS equipment coverage for EFTS equipment located off premises.
- An extension of Bankers Blanket Bond coverage to each Automatic Teller Machine (ATM) on the network.
- Liability insurance coverage for each ATM location.

Insurance coverage at the serviced institution should furnish protection from loss, because of employee dishonesty in the servicer's organization. Standard Form No. 24, "Bankers Blanket Bond," provides fidelity coverage of the data servicer's employees unless specifically excluded by a separate rider. A premium is charged for each processor. Transit Insuring Agreement © of Form 24 covers some of the costs associated with reconstruction of accounts and other records if lost or destroyed during transport by the financial institution's messenger. Additional "Cash Letter," "Valuable Papers," and "Records" coverage may be appropriate.

MANAGEMENT APPRAISAL

Generally, a direct relationship exists between the overall condition of the IS resources and the quality and size of its management and staff. An evaluation of management should consider its performance and planning for future needs.

The examiner should evaluate the staffing, supervision, management responses to correct cited deficiencies from audit and examinations, and control for each area reviewed. Strengths and weaknesses as summarized in the work program (see Chapter 9WP: Management Work Program) should also be considered. Generally, a review of IS in a financial institution or independent service bureau includes a review of financial condition, audit, computer operations, systems development and programming, personnel policies, management succession, and employee training.

Management succession is a legitimate concern of any organization and is perhaps even more important in IS processing. It is to the institution's advantage to employ those who with experience and training could advance to management positions. A financial institution should avoid depending upon one person or several key personnel. Provisions should be made for continuing operations in the event of an unexpected loss of key personnel. Education

programs, including management training for supervisors, can minimize disruptions to operations from management or staff turnover.

Management's ability to administer effectively all aspects of the IS function and to interact with user groups and other managerial personnel within the organization are keys to the success of any data processing operation.

MANAGEMENT INFORMATION SYSTEMS (MIS)

Effective MIS reports are critical to the profitability, success, and long-term viability of each institution. For management and the board of directors to make informed decisions, they must have information systems that provide the necessary information needed to run their business. They must be provided with accurate, timely, and consistent information on the institution's performance, management of its resources, and compliance with regulatory requirements.

A critical factor in reviewing management is the quality of the institution's management information systems. Effective MIS consists of information drawn from a number of sources. Although the concept of quality MIS is accepted widely as a requirement for success, it is difficult to define since MIS requirements are unique to each institution. Examiners should direct their efforts to evaluate MIS by:

- Determining if management has adequately identified information requirements and established effective reporting information to guide their decisions in achieving business goals and measuring performance. Generally, the review of MIS will be facilitated by focusing on a specific safety and soundness concern (i.e., profitability, asset quality, interest rate risk, regulatory reports, such as call reports, thrift financial reports) or compliance issue (i.e., Community Reinvestment Act, and Bank Secrecy Act). The IS examiner must work closely and concurrently with other examiners (e.g., safety and soundness, compliance, trust, or holding company) in reviewing the quality of MIS reporting information at an institution.
- Reviewing MIS reports to determine the accuracy and timeliness of the information provided, and the controls that ensure that it is reliable, timely, accurate, and treated with confidentiality.

Advances in technology have increased the amount of the information available to management and the board of directors for planning and decision-making. These advances have also increased the potential for inaccuracy and errors in management reports. Data may be extracted from numerous transaction and financial systems that run on mainframes, minicomputers, and microcomputers without the benefit of well-designed processing controls commonly found in traditional mainframe systems.

An institution's information requirements depend on its size and the complexity of its operations. Directors and management need information to define goals, guide operations, and make timely decisions. Although examiners should encourage management to develop improved systems and information, they must be reasonable in their expectations. They should encourage institutions to recognize their information needs and take steps to develop the systems to address them.

Management information is required at all levels of the institution. The information at each level may vary according to management's responsibilities. The effectiveness of MIS can be measured in terms of quality, quantity, and timeliness. Examiners must determine if an institution's management information systems provide the type, quantity, and quality of data necessary to assess and monitor its performance.

The following factors may be used to evaluate the quality of the institution's management information systems:

- *Usable* – Decision makers need summarized information. Reports should be designed to eliminate clutter and voluminous details that can create information overload. Care should be taken that board and management reports present only relevant information and do not contain unnecessary detail. The volume of detail in board reports can prevent directors from recognizing potential risks that are more visible in summarized information.

- *Timely* – Current information should be available for decisions. Management information systems should be designed to expedite the reporting of information. Procedures should be designed to collect and edit data, quickly summarize the results, and allow for adjustments and corrections.

- *Accurate* − A sound system of automated and manual internal controls must exist throughout all information systems processing activities. Information should receive appropriate editing, reconcilement, and internal control checks. A comprehensive internal and external audit program helps ensure the adequacy of internal controls.

- *Consisten*t − Data should be processed and compiled the same way each time. Variations in how data is collected and reported can distort information and trend analysis with adverse effects on management decisions. Since data collection and reporting processes change over time, management must establish sound change procedures. The change procedures should be well defined and documented, clearly communicated, and contain an effective monitoring system.

Comments on MIS reports should be specific, rather than general. Management at various levels needs specific information to understand the nature of the deficiency and how to correct it. When making comments examiners should consider :

- Why the MIS report is inadequate. Whether the information provided is timely, is in a useful format, is complete or sufficiently detailed, or is properly organized. Whether the information requires reference to several other sources to be useful.

- That references to specific reports contain a copy of the report with the name and number. Problems are highlighted from the standpoint of the users of the report, not the examiner.

- Whether the report is generated on the mainframe or on a PC within one department. The institution's information systems department cannot fix a report that it does not know exists.

- That if the report is generated within a department, why is it done that way. Whether the accuracy was checked and how.

- Whether the institution has custom report writers and on-line inquiry capability and the audit department commonly uses these programs. The use of custom report writers before the examination can save time during the examination by allowing the examiner, with the help of the institution, to design reports that provide needed information in a useful form.

Because management requires information on economic events that may occur, the use of *models* has become more prevalent. Assumptions made and the quality of information used in models may have a serious effect on the value of the information gleaned from them. Therefore, controls over morels should be sufficient to ensure that management receives accurate information to make proper decisions.

OUTSOURCING DATA PROCESSING SERVICES

The intense competition in the financial services industry has caused institutions actively to seek ways to cut costs and focus on the business of banking. At the same time, the rapid changes in information systems technology have increased the costs of developing and maintaining in-house and end-user information systems significantly. As a result, many financial institutions have contracted with third-party organizations for information processing, telecommunications, item processing, or other selected services. These arrangements generally are referred to as *outsourcing*. Outsourcing is done to reduces operating expenses by removing salary and equipment expenses from the institution's books and allocating the savings in capital to core business needs.

Outsourcing arrangements permit the institution to focus on the business of banking and rely on the servicer to provide state-of-the-art systems in compliance with regulatory requirements. Longer term outsourcing contracts also permit the institution to predict its data processing costs with a higher degree of certainty as the servicer bears the costs of technological changes. The vendor achieves cost

savings and economies of scale by consolidating and reducing data processing facilities, computers, and software maintenance activities. Institutions should ensure that long-term strategic plans are considered in long-term outsourcing contracts.

Outsourcing arrangements generally fall into three categories:

Service Bureau Arrangement

The institution contracts with a servicer to provide data processing systems and services on proprietary software applications used by a number of clients. It may contract out all or some of its applications as it chooses.

Facilities Management (FM)

The institution turns over management of its data center facilities to a third party. The installation is customized to meet its needs. Operating system support is generally the responsibility of the FM provider. The facility housing the computer and the computer equipment is often owned/leased by the institution.

Resource Management

The vendor processes and maintains the institution's software applications at its data center or may install new applications on a dedicated computer. A major difference between a resource management and service bureau arrangement is that, in the latter, the institution uses the vendor provided software applications instead of its own. Current knowledge of software systems is a major factor in outsourcing decisions. Institutions must consider the costs and resources involved in upgrading legacy or early application software systems and maintaining competitive software on mainframe and end-user computing systems.

Outsourcing arrangements often result when management views data processing as one of many functions of the institution. The maintenance of current technology on in-house computer systems may drain profits when institutions are seeking ways to cut costs. Other factors that affect the outsourcing decision may be earnings pressure, possibility of acquisition, internal structuring/decentralization, and the perception that third-party vendors in the information systems business are better equipped to maintain state-of-the-art technology at lower costs. These views are not shared uniformly throughout the financial institutions industry.

A management that pursues outsourcing risks the non-performance of a careful comparison of in-house cost with third-party costs. Review of that analysis leading to the outsourcing arrangement is important for safety and soundness. An evaluation should be made about whether the institution relied solely on the marketing data of vendors or reconciled its system requirements to various outsourcing proposals.

A more difficult area for an institution to evaluate is the cost and benefit of an outsourcing agreement. Some reasons are:

- There are no cost accounting standards in the financial institutions industry. Some institutions spread data processing cost throughout the organization, while others track cost centrally. Thus, the value of any industry data on the average cost of data processing in financial institutions is limited.

- Products and services of outsourcing vendors are priced and packaged differently than in-house data processing operations. Vendor software packages and processing are proprietary and offer different advantages and disadvantages. They are not a homogeneous grouping of products and services and cost comparisons among vendors, and vendors and in-house operations can be misleading (e.g., cost per deposit account).

- The correlation between cost and benefit of an outsourcing agreement is not always identified and quantified. For example, lower data processing costs may be accompanied by higher personnel costs in user departments and lower quality in customer service.

Contracts also should be reviewed carefully by management when considering an outsourcing arrangement. Some considerations are security, ownership of the data stored on vendor media, and the right of the institution to recover its data upon expiration or termination of the contract.

In a typical outsourcing arrangement, the financial

institution signs a contract giving the vendor control of its computer operations for several years. However, the contracts are generally structured, so that the savings for the institution accrue almost entirely during the first few years. Some outsourcing transactions are designed to provide immediate financial relief by having the third party vendor take over the IS equipment and personnel to remove these expenses from the institution books.

The provision of IS services to financial institutions entails certain risks and responsibilities for both the financial institution and the vendor. IS services and systems contracts should address, define, and balance those risks and responsibilities between the vendor and the institution. Guidelines that institutions should consider when contracting for data processing services and systems are provided in the FFIEC issuance SP-6: Interagency Statement on EDP Service Contracts, the OCC issuance BB-87-3: Potential Risks of Long Term EDP Contracts, and the OTS issuance TB-46: Contracting for Data Processing Services or Systems. Additional Serviced Institution Control Guidelines are also provided in Chapter 22.

SYSTEMS CONVERSIONS

Financial institutions must replace periodically existing software applications with new ones developed in-house, or more likely, with vendor software, either through a leasing or outsourcing agreement. The replacement is accomplished through a systems conversion process. These conversions present significant risks of loss to the institution from deficiencies in planning and implementation. Losses incurred often arise from charge-offs resulting from discrepancies between pre-conversion and post-conversion monetary balances, extensive efforts to resolve out-of-balance conditions and to work around unresolved transaction processing deficiencies, and indirectly, negative customer impact. Because individual institutions perform conversions infrequently, its employees do not usually possess conversion expertise. Thus, an inordinately large degree of reliance is often placed on software vendors who, tend to present an over-optimistic view of the effort required to complete a conversion to their system. As a result, conversion-related risks are often increased significantly by implementation efforts performed under unusually tight schedules. Consultants, when engaged, are often hired at relatively short notice. This tends to inhibit their overall effectiveness in guiding the project.

The IS examiner's review should identify potential or actual problems to help avoid loss or major disruption to the institution. It should determine the adequacy of the institution's preparedness for a scheduled systems conversion. To be of most value, the review should be started no sooner than the completion of the planning phase and no later than the middle (approximately) of the user acceptance testing phase. In general, institution management prefers reviews of systems conversions to occur early in the process to take advantage of the reviewer's findings and recommendations. The early detection of significant safety and soundness risk exposures, may be assured by reviewing system conversions in targeted rather than regularly scheduled information systems examinations. This examination may involve in-house data centers, serviced institutions, or service bureaus and should be conducted only by experienced IS examiners.

The IS examination scope is divided into the conversion plan and implementation controls and progress achieved relative to the conversion target date. Each phase has the following features:

- Conversion plan: In most respects, planning for a conversion is similar to that of planning for any systems development effort. All tasks must be identified and executed according to a defined critical path, and personnel and other resource requirements must be provided for to complete the conversion within a designated target date. However, planning for a conversion requires that provisions be made for certain tasks that are uniquely associated with the transfer of processing from one existing system to another. These include file conversion and related balancing procedures, product mapping, data mapping, and the selection of system user options. Planning for these tasks should be reviewed along with that of other tasks that correspond with typical systems development projects including system procedures, user training, and the implementation of disaster recovery planning and information security controls.
- Implementation: An implementation phase review allows examiners to evaluate all aspects of

planning and project management, including an assessment of the progress achieved against task completion target dates. Red flags that portend conditions of high risk exposures include:

Conversion target date:
- Arbitrarily set.
- Management appears firmly opposed to postponement.
- Previous target date(s) missed.
- Conversion team is performing under evident time pressure.

Project management:
- Completion of key tasks and milestones significantly delayed.
- Critical path-dependent tasks are started prematurely (e.g., user acceptance testing is started before the completion of the selection of system user options).
- Project management records are not kept updated.

Testing:
- Planned time frames for testing are shortened.
- The is no evidence of independent review of test scripts for adequacy.
- Deficiencies are identified initially as conversion- critical (show stoppers), are arbitrarily reclassified as noncritical, and are to be corrected after conversion (usually to meet a target date).

Procedures and training:
- Balancing and user procedures are not adequately completed.
- Inadequate progress is made in user training.

Network:
- Network connectivity to the new vendor's facilities is not tested adequately.

EMERGING TECHNOLOGIES

The rapid growth of IS technology is changing business operations in financial institutions. The demand for increased features and functionality of information systems, reliable and timely information, and the reduction of paper have prompted vendors to design a wide range of technical solutions to meet business problems. Advancements in the spread of the Internet, client-server architecture, distributed networks, Fourth Generation Language (4GL) programming languages, storage technologies, expert systems, and electronic data interchange (EDI) have aided the transfer of computing power from centralized computers to end-user computing platforms.

This proliferation of emerging technologies in information processing has created new risk and control issues for the institution and for its regulatory agencies. Institutions are experiencing an increased volume of data, speed of processing, on-line reporting capabilities, complexity of business processes, and user controlled processing. These changes have increased user access to information systems, reduced segregation of duties, caused a shift from paper to electronic audit trail, evolved with a lack of standards and controls for end-user systems, and increased the complexity of corporate contingency and IS recovery planning. Accordingly, the board of directors and regulatory examination personnel must ensure that the risks related to emerging technologies are considered and addressed appropriately by the institution's management. Some emerging technologies that are becoming more prevalent in financial institutions are discussed next.

THE INTERNET

The Internet is the world's largest computer network, but there is no easy way to characterize its size. An estimated 1.2 million computers were connected to the Internet at the beginning of 1993. However, the Internet does not count its membership solely in terms of either computers or computer users. Internet membership also includes networks. Today hundreds of thousands of local networks are connected to the Internet, and its rate of growth is increasing steadily. Roughly 1,000 new networks join the Internet each month. Even new networks do not account for all of the Internet's growth. The Internet's audience expands with every new computer or user that is added to any of its constituent networks.

Origin of the Internet

The Internet had a humble beginning as ARPANET in the early 1970s. The ARPA part of ARPANET stood for Advanced Research Projects Agency (later

called the Defense Advanced Research Projects Agency, or DARPA) of the U.S. Department of Defense (DOD). At the end of the 1970s, other networks sprang into existence. The UUCP (Unix to Unix Copy Protocol) network (a loose confederation of first hundreds and now thousands of UNIX machines) was followed in the early 1980's by BITNET (Because It's Time Network), CSNET (Computer Science Network), and many others. Some were private (such as CERFnet and BITNET), some were collaborative (UUCP), and some were government funded (ARPANET, NSFNET [National Science Foundation], and CSNET). Eventually all of these networks began working together and became known as the INTERNET.

This evolution was begun by the National Science Foundation (NSF), which created a network of interconnected NSF supercomputer sites across the United States in the late 1970s and early 1980s. NSF is a government science agency that connected supercomputer sites to each other to make them more efficient. Scientists, researchers, and engineers could network across the supercomputers and better leverage the agency's computing power.

The high-speed network that connects the NSF supercomputers now forms the backbone of the Internet in the United States. It consists of high-capacity telephone links using microwaves, lasers, fibre optics, and satellites to connect networks, computer sites, and people around the world.

As the Internet has become more visible outside of the research and academic communities, a group of private companies called service providers have evolved. These service providers actually furnish many of the entry point communication lines used by Internet users. Universities, private research labs, and commercial companies rent Internet connections from these providers, as an individual would lease a telephone line from the phone company. The advent of Internet service providers (ISP's) geared to the individual home or small business user community opened up the Internet more fully in the early 1990s.

What Can Be Found on the Internet

The primary growth area for electronic commerce, including banking, is a portion of the Internet called the World Wide Web. The World Wide Web interest commercial enterprises, because it allows users, with necessary navigator software, to display their products graphically and to link to related information merely by pointing and clicking on a highlighted word or phrase.

Searching for information on the Internet is not always easy. There are many tools to help a user find information on the World Wide Web (WWW or The Web) portion of the Internet. These tools, often referred to as browsers, web crawlers, or search engines, allow the user to find topics on the Internet using graphical point-and-click interfaces. The Web puts a friendlier face on the technical aspects of navigating the Internet. The technical complexity of the Internet was a primary reason that it was not noticed much until recently by the public and private enterprise. Currently the most widely used part of the Internet is electronic mail (E-mail).

Organization

The Internet is a loosely structured, informal association of computers connected by networks, whose only mandatory control is the *address* or *network name* of each network site. Without proper controls on the network name, it is not possible to accurately switch or route messages. Therefore, controls on the network name are the fundamental glue that both define and hold the Internet together. The Internet Activities Board (IAB) has this responsibility. The IAB is supported by the Internet Society, a private nonprofit organization of individuals and organizations that are connected to the Internet.

Components

The Internet is comprised of:

- *Computers* – which represent the host locations on the network and can range from a freestanding microcomputer, to a LAN server, minicomputer, or a mainframe.

- *Networks* – which represent the paths over which communications travel between the Internet nodes.

The diversity of hardware and software and the range of processing power of these computers and networks is the source of the Internet strength and its weakness.

Internet Banking

Internet banking creates new challenges. Customer terminals and the delivery channels (e.g., public telephone networks and the Internet) are outside of the institution's control. The global reach of these systems increases the number of uncontrolled points of access to bank computer systems. These attributes introduce heightened security risks and emphasize the need to develop secure systems and procedures for operating in an uncontrolled environment.

An evaluation should be made of risks associated with existing or proposed PC banking programs in terms of all significant technology, legal, regulatory, and economic areas. The following factors warrant special consideration followed by appropriate action:

- *Accountability* – Ensure that proper accounting, audit trails, and operational controls are in place and operating correctly. These controls are normally available in a traditional information systems environment; however, the challenge exists in the ability to monitor and trace the increased transaction volume of more users that accompanies PC banking.

- *Authentication* – Verify the identity of the parties to the transaction. Financial institutions will communicate with customers they may never physically meet and opportunities for misrepresentation will increase. Financial institutions and customers will need a mechanism to verify each other. Authentication is one of the most significant issues related to PC banking.

- *Authorization* – Develop methods, before implementing PC banking, to ensure that customers are authorized access only to their accounts and to perform only pre-determined and legally permissible functions.

- *Capacity* – Acquire and allocate sufficient resources to meet existing and anticipated volume. Customer will expect access to their financial data and the ability to conduct transactions on demand. During peak operating hours, demand may be high and unpredictable.

- *Confidentiality* – Keep customer data safe from unauthorized access. Customer data will be transmitted over public networks. Management must develop methods to maintain privacy.

- *Human Resources* – Ensure there are sufficient trained personnel to supply prompt and expert customer service. All affected employees will need training appropriate to their responsibilities.

- *Information Integrity* – Confirm that data remains accurate and safe from illegal alteration. Customers will enter data in an on-line environment. Management must assure that data transmissions between the customer and the financial institution remain protected from unauthorized viewing or alteration.

- *Non-Repudiation* – Create a system that will provide undeniable proof of participation by both the sender and the receiver of information and data in every on-line transaction. Customers may input data and later deny the transaction took place. Authentication is the primary component of non-repudiation.

- *Outsourcing* – Select only vendors who demonstrate in-depth knowledge and effective use of the emerging technology. Many service bureaus and software vendors will offer to develop and distribute PC banking services. These will include new unproven vendors and established vendors, both of whom may be unfamiliar with the technology and its implications.

- *Reliability* – Ensure that every part of any system used by the bank is available and functions as promised and establish contingency plans for emergencies. Contingency planning is necessary to restore an on-line system that fails and to provide continuity of business activity. Internet reliability is a related concern, but management has little or no control over Internet performance.

- *Software Updates* – Maintain control over software changes. The institution may have to rely on the customer to install software updates. Multiple software versions may have to be supported. The institution must decide what software versions to support and how to accommodate customers unable or unwilling to install updates.

- *Compliance* – Ensure compliance with all legal and regulatory requirements. The existing regulatory framework remains applicable in this emerging technological environment and must be adhered to.

Internet Issues

This area of technology has developed so rapidly that its coverage by current law and regulations is unclear. Many of the laws, rulings, and regulations were under review as we crafted this section. Accordingly, readers should continue to monitor legal developments associated with banking on the Internet. Of particular concern are issues related to error resolution, including: data corruption and

unauthorized transactions; protection of individual privacy; and safeguards against illegal activity. Such safeguards would address particularly the areas of money laundering and fraud.

Actual financial activity on the Internet (or through on-line, services such as America Online, Compuserve, or Prodigy) may take various forms, including:

- Institutions only providing product information on line with referrals to telephone or branch sites for transactions.
- Customers obtaining account status information.
- Customers conducting transactions on existing accounts, (including transferring funds and making payments).
- Institutions providing information about uninsured products and financial planning information.
- Customers initiating the purchase of securities or other uninsured instruments on-line.

Similar services may be delivered through direct dial-up, using branded interfaces provided by the institution or through the use of third-party software, such as provided by Intuit, Microsoft, or MECA.

Numerous issues surround the role of third parties, such as: on-line services, Internet providers, and intermediaries processing financial transactions (such as Intuit, Microsoft, and Checkfree.). Because agent/principal relationships are often defined by applicable state law, no precedent exists for transactions conducted on an interstate or international network by parties whose the geographic location may be unknown. Handbook readers should monitor developments in this area.

Compliance Related Risks and Issues

Internet banking transactions should be subject to the same compliance laws and regulations that apply to "traditional" banking transactions. The application of those laws to Internet banking transactions raises questions, such as compliance with advertising requirements and the provision of timely disclosures in an appropriate form. Financial institutions could risk regulatory enforcement and civil penalties for noncompliance with those laws and regulations.

Depending on the type of transaction that occurs (for example, extension of credit or deposit or withdrawal of funds from an account at a financial institution), the following federal laws and regulations could apply:

- Equal Credit Opportunity Act and Federal Reserve Regulation B

  Prohibits discrimination by creditors in any aspect of a credit transaction on a prohibited basis and requires creditors to provide certain notices concerning credit applications.

- Fair Housing Act

  Prohibits discrimination by any aspect of housing-related lending on a prohibited basis.

- Home Mortgage Disclosure Act and Federal Reserve Regulation C

  Requires depository institutions and mortgage lending institutions to report data on mortgage loan applications, originations, and purchases.

- Electronic Fund Transfer Act and Federal Reserve Regulation E

  Requires financial institutions to provide disclosures and consumer protections (such as error resolution procedures and limitations on liability for unauthorized transfers) concerning electronic fund transfers involving a consumer account.

- Truth in Lending Act and Federal Reserve Regulation Z

  Requires creditors to provide disclosures (including in advertisements) and consumer protections (such as error resolution) in consumer credit transactions.

- Expedited Funds Availability Act and Federal Reserve Regulation CC

  Requires financial institutions to make deposited funds available to customers within specified time frames and to provide disclosures about funds availability policies.

- Truth in Savings Act and Federal Reserve Regulation DD

  Require depository institutions to provide dis-closures (including in advertisements) and consumer protections (such as calculation of interest on the full account balance) concerning deposit accounts.

- Community Reinvestment Act and Federal Reserve Regulations

  Require federal financial regulatory agencies to assess

the record of regulated financial institutions in meeting the credit needs of their entire communities, including low- and moderate-income areas, consistent with safe and sound practices.

To ensure a consistent regulatory policy approach to Internet banking. The following issues should be addressed.

- Appropriate triggers for existing advertising requirements may need to be created for on-line interfaces.
- Standards may need to be set for, if, and when it is appropriate to use on-line disclosures, periodic statements, and notices rather than sending hard copies.
- Similarly, a review may be indicated of the situations in which E-mail communications would appropriately substitute for communications between the institution and a customer.
- Rules for providing disclosures, statements, and notices within certain time frames should be adopted and evaluated for the on-line transmission.
- Whether continuously available real-time statements could substitute for, or issued in lieu of, periodic statements should be considered.
- When downloadable documents and E-mail would be considered a form the customer can retain, as required for certain disclosures, etc. should be resolved.
- Standards should be developed for documents that must be delivered to the consumer, to ensure that they have been received and downloaded both accurately and in their entirety.

Marketing and sale of securities and other uninsured instruments through an institution's Internet site can also potentially raise additional compliance issues.

Institutions have not been sensitive as necessary to the need to separate banking from nonbanking activities, even without direct links to the brokerage provided by Internet browser technology and incorporated into on-line banking interfaces. While the actual securities transactions are covered by SEC rules (which has approved on-line delivery of the prospectus and/or the sale of securities), interface standards should be established to distinguish activities involving uninsured instruments and maintain and reinforce separate corporate identities.

Geographic Issues

Issues related to Internet banking fall into two primary categories: those for institutions using this technology to supplement ordinary banking activities and those for institutions doing business solely on-line.

For the first category of institutions, Internet banking provides an *alternative* delivery system for banking products and services. Access issues may arise over the availability of computers to low- and moderate-income populations. The implications of this are covered in the discussions of automated application systems and retail electronic payment systems. The obvious potential for on-line banking is to concentrate an institution's business in the high end or the market. Furthermore, its geographic independence from an institution's offices provides the potential for an institution to concentrate business outside of its more traditionally identified trade area.

For the second category of institutions, Internet banking provides a *primary* delivery system for banking services. An institution doing business solely on-line could be subject to issues related to computer access by low- and moderate-income segments of a community.

The cornerstone of many laws affecting financial institutions is the concept of a local community, in which the institution is expected to meet the needs of all segments, including those of low- and moderate income persons. Many legislative initiatives address geographic location. Given that an institution doing business on-line could be considered to have an office located wherever any customer has a computer, a different strategy for defining its trade areas may need to be established.

The Internet's Future

The Internet's future as a primary delivery system of financial services is evolving rapidly. Financial institutions using or planning to use the Internet as a financial services delivery mechanism will also continue to develop policies, standards, and procedures internally or collectively to protect their assets and the overall integrity of both their systems and transactions traveling across the Internet.

CLIENT/SERVER COMPUTING SYSTEMS

Client/server networks enable users to share computer resources across all computing platforms of an organization (workstations, PCs, mid-range computers, mainframes). Portions of a single application may be split between the client workstation or PC and the server based on the most effective or efficient use of equipment. A server may be one or more multi-user processors with shared files that serve multiple clients simultaneously to provide printing, facsimile, file storing, database,

computational capabilities, and application processing.

Client/server technology allows organizations to increase worker performance by distributing computing resources and empowering the end user. End users have more input into the design, development, and implementation of new systems. They are now considered to be owners of the data. As owners, they are responsible for data integrity, including security concerns that were only related to the mainframe. In some cases, users of information evaluate, purchase, test, and install powerful programs on their own systems. These user systems may interact with, alter, or replace information processing performed on mainframe computers.

A general area of concern in client/server systems is the adequacy of general computer control procedures. Risk issues in that environment include:

- Data and security issues across platforms in multiple locations with multiple access points.
- Mismanagement of end-user computing.
- Development, maintenance, and testing of new applications.
- Back-up and recovery procedures.
- System integrity affected by lack of controls in end-user platforms.
- End-users inadvertently or deliberately modifying or destroying data.
- High-volume PC use, increasing the possibility of system failure.
- Viruses entering the system.
- Changes in one vendor's hardware affecting other vendor components.

ELECTRONIC IMAGING SYSTEMS

Electronic document imaging systems provide a combination of hardware and software technology to capture, index, store, and retrieve electronic images of paper documents. They are used by financial institutions to reduce paper handling, increase productivity, and improve customer service.

Although the image capture process (scanning) is still in its infancy, the technology is improving and will provide high speed data capture, indexing, reliable optical character recognition, storage, and networked data exchange. Document storage technology is also improving and data storage on write-once-read-many (WORM) and rewriteable optical disks is becoming an integral component of many image systems. The optical disk is a storage device that uses laser technology to retain digitized data from any means of data input, including scanning. The optical storage disk technique is an outgrowth of the demand for higher levels of document storage capacity in a usable form. This new digital media offers a highly reliable and low-cost process for the storage and access of imaged documents and other types of data on a compact optical disk. Imaging systems may streamline department and office workflow processes, reduce storage and retrieval costs, and by automate customer files and correspondence. The replacement of paper documents with electronic images can affect significantly the way 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.

Imaging systems generally are grouped into two types: Document management systems and item processing systems. Imaging systems and accompanying risk and controls issues are described in Document Imaging – Chapter 17 and are also referenced in FFIEC SP-10 – Control and Security Issues in Electronic Imaging Systems. This FFIEC policy issuance is located in Chapter 2 of this Handbook.

ELECTRONIC DATA INTERCHANGE (EDI)

EDI refers to the electronic exchange of documents and other data between corporations. Companies exchange documents by direct transmission between computers over telephone lines and data communication links. Data files are transmitted in a standard format that is machine readable by the computer receiving the files. The initial users of EDI were large companies who used communication links and a proprietary transmission format to exchange data with their suppliers and customers. New standard protocols allow customers with different equipment and software to send and receive messages in a standard message format. These messages can be translated and entered directly into the computer system at the destination in an electronic form.

The EDI goals are to lower cost, improve accuracy in billing and inventories, speed cash management, and assure quality control. EDI provides savings in time, postage, and paper by eliminating the mailing of paper documents. It also replaces keying data into a computer from paper documents, at the destination organization,

saving data entry time and reducing keying errors.

The growth of the EDI process has led to the development of transmission standards and value-added networks (VANS). VANS are third-party networks that store and forward messages in a standard format. They serve as electronic mail boxes and provide EDI partners with the flexibility to choose when to access or transmit information. VANS help to reduce scheduling and compatibility problems associated with automated transfers of information between multiple companies.

EDI software generally has three phases: communication, translation, and application interface. A complete message, such as an order invoice, would comprise an EDI transaction. The communication interface transmits the message between the companies or VAN and is designed for error detection and correction to protect against transmission failures. An EDI translator converts the standard EDI messages into proprietary user formats and performs edit checks, response acknowledgments, and validity checks. The application interface converts the information into a format that can be processed by the receiving application software. Usually, the company's software applications are left unchanged.

Financial institutions have been involved primarily with the electronic payment portion of EDI transactions through electronic funds or ACH transfers. These services include wire transfer, automated cash management, and ACH transfer services for the participating companies. The types of ACH transactions involved in the EDI payment process are: prearranged payments or deposits, corporate trade payments, and corporate cash concentration and disbursement transactions. Financial institution customer charges are generally based on a set-up fee, a monthly maintenance charge, and a transaction charge based on the number of characters in EDI transactions.

The greatest risk to financial institutions lies in the electronic payment transaction. Exposures and risk associated with payment system risk apply to EDI transactions. Financial institutions bear a credit risk if payment is made from accounts with uncollected or insufficient funds. Credit limits and transactions caps should be established, periodically reviewed, and strictly enforced.

Since EDI replaces paper with electronic entries, many of the manual process controls are either lost or ineffective. Examples include the substitution of electronic signatures and authorizations to replace written documents. Audit trails, access controls, security and separation of authorization, and execution and data processing functions must be designed into the technology. Backup and restart procedures are necessary to recover operations and assure their continuity. Legal requirements place a need for security and the ability to ensure data integrity. This may require that copies of printed documents be retained to defend against legal suits alleging improprieties in handling the account, or even fraud.

Legal considerations include:

- Proof of authentication.
- Record retention.
- Contract law covering written agreements
- Control regulations stipulated by the Foreign Corrupt Practices Act:
  - Executing transactions in accordance with management's general or specific authorization.
  - Recording transactions to allow for the preparation of financial statements.
  - Controlling access to assets.
- Transactions governed by Federal Reserve's Regulation E.

The following tax regulations and rulings also govern EDI transactions.

- Revenue Ruling 71-20 requires that the media be retained for as long as it would be useful to determine a tax liability.
- Revenue Ruling 86-19 assumes the existence of underlying source documents to support inter-company transaction systems.

This section is intended to determine if the organizational structure, the resources, and the control policies and procedures are adequate to foster effective information support. It will also address the quality of management and supervision of the data processing activity, including management's administrative process. The examiner should document findings especially those that do not satisfy the recommendations outlined in the *1996 FFIEC IS Examination Handbook*. This document will be included in the workpapers.

ORGANIZATION

1. Review the corporate and Information Systems (IS) departmental organization charts to determine if:

    a. The organizational structure provides for effective IS support throughout the organization.

    b. IS management reports directly to senior level management.

    c. The IS department has maintained its independence from user departments.

    d. Appropriate segregation of duties is provided.

2. Review biographical data of key personnel and the established staff positions to determine the adequacy of:

    a. Qualifications.

    b. Staffing levels.

    c. Provisions for management succession.

3. Review and evaluate written job descriptions to ensure that:

    a. They are maintained in writing and are updated promptly.

    b. Authority responsibility and technical skills are clearly defined.

4. Test key positions to determine if the job descriptions are reasonable and represent actual practice.

5. Review IS department personnel separation procedures for adequacy.

6. Determine if management provides an adequate orientation and continuing education programs.

7. Determine the adequacy of the compensation program and its effect on staff retention or turnover.

8. If IS employees have duties in other departments, determine if:

   a. Management is aware of the potential conflicts such duties may cause.

   b. Conflicting duties are subject to appropriate supervision.

PLANNING

9. Obtain or prepare a list of board, IS steering, or relevant management committees that meet regularly to review IS related matters. Indicate the title of each member and determine if IS group, user community, and audit are well represented.

10. Review the minutes of the board of directors and relevant committee meetings for evidence of senior management support and supervision of the IS activities.

11. Determine if committees review, approve, and report to the board of directors on:

    a. Short-, and long-term IS.

    b. IS operating standards, including computer security and data security standards and procedures.

    c. Resource allocation (e.g., major hardware/software acquisition and project priorities).

    d. Status of major projects.

    e. IS budgets and current operating cost.

    f. Research and development studies.

g. Corrective actions on significant audit deficiencies.

12. Determine if the board of directors or senior management gives adequate consideration to the following IS matters when formulating the institution's overall business strategy:

    a. Is strategic plans.

    b. Current status of the major projects in process or planned.

    c. Staffing levels.

    d. IS operating costs.

    e. IS contingency planning.

    e. Institution business recovery planning.

13. Review the strategic plans for is activities. Determine if the goals and objectives are consistent with the institution's overall business strategy. Document significant changes recently made or planned that affect the institution's organizational structure, hardware/software configuration, and overall data processing goals.

CONTROL

14. Determine if IS management has adequate standards and procedures governing:

    a. Personnel administration.

    b. Systems development and support functions.

    c. Computer operations.

    d. Telecommunications network operations.

    f. Computer and information security.

    g. Contingency planning/disaster recovery.

15. Determine if the standards and procedures outlined in step 14 address:

a. Adequate segregation of duties.

b. Limiting access to sensitive information system resources (e.g., magnetic media, documentation, and computer equipment).

c. Ensuring authorization of all activities within the is area.

d. Creating sufficient audit trails that would allow independent verification by the user groups.

16. Determine the effectiveness of the reports used by senior management or relevant management committees to supervise and monitor the following IS activities:

    a. Management reports that provide the current status of software development/maintenance activities.

    b. Performance and problem reports prepared by user groups.

    c. System use and planning reports prepared by operating managers.

    d. Internal and external audit report of IS activities.

17. From management reports, measure actual performance of selected major projects against established plans. Determine the reasons for the shortfalls, if any.

18. Determine if management has taken positive action toward correcting exceptions reported in audit and examination reports.

FINANCIAL ANALYSIS

19. Analyze financial statements and IS operating costs to determine:

    a. Cost allocation method.

    b. That cost allocation methods applied are similar for both affiliated and non-affiliated customers.

    c. The significance of IS revenues from non-affiliated users relative to the institution's overall financial condition.

d. If fees charged affiliated customers are reasonable.

e. If the institution has a contingency plan to provide for the loss of revenues from the non-affiliated sources, where significant, through competition or technological changes.

20. If the servicer is not a financial institution, list:

a. Ownership, naming owners of 5 percent or more of the stock.

b. The members of the board of directors, indicating:

- Name.
- Occupation.
- Principal business affiliation.
- Relationship with other affiliates of this institution, if applicable.

21. If the institution receives significant outside data processing support, as identified in step 5 of the Examination Planning section:

a. Provide the name and location of the servicers. Include any known affiliations with financial institutions or is vendors.

b. Determine that the services are covered by a formal written service agreement.

c. Determine if the agreement is directly with the servicer or through a third party. Identify the third party, if applicable.

d. Determine if the institution has reviewed the current financial condition of its IS servicer.

e. Determine that management has requested from its regulator information on the most recent examination of its service(s).

22. Based on the information available, determine if any servicer raises concern, because of financial weakness or inadequate operational controls. If such concern exists:

a. Determine if conditions have been satisfactorily resolved.

b. Determine what action has been taken to correct the conditions.

c. Determine if management has identified or secured alternative sources of IS support if conditions are not corrected within the specified time frame.

23. Review the adequacy of insurance coverage (if applicable) for:

a. Employee fidelity.

b. IS equipment and facilities.

c. Media reconstruction.

d. EFTS activities.

e. Loss resulting from business interruptions.

f. Errors and omissions.

g. Extra expenses, including backup site expenses.

h. Items in transit.

i. Other probable risks.

SYSTEMS CONVERSIONS

24. Review the systems conversion, controls associated with its implementation, and implementation progress achieved relative to conversion target date and:

a. Project management records.

b. Minutes of conversion team meetings.

c. Internal and external correspondence pertaining to the conversion.

d. File conversion balancing procedures and results of file conversion tests.

e. Evidence of successful completion, as applicable, of product mapping, data mapping,

system user options selection, user acceptance testing, user procedures, and user training.

f. Proof of successful testing of network connectivity to the new vendor's facilities and adequate progress in implementing new vendor-related disaster recovery plan and information access controls.

CONCLUSIONS

25. Review the results of work performed in this section and in sections for Planning and Audit. If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

26. Summarize the strength and weakness of the condition of IS activities in this area.

27. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

28. Assign rating (see Chapter 5 for additional information).

29. Provide any additional information that will facilitate future examinations.

Examiner | Date

_____|_____

Reviewer's Initials

CORPORATE CONTINGENCY PLANNING

CHAPTER 10

(FILE NAME ON DISK # 1 = S2C10.WPD)

The board of directors and senior management are responsible for establishing policies, procedures, and responsibilities for organization-wide contingency planning. The institution's contingency plan should address all critical services and operations which are provided by internal departments and external sources. The plan should be a coordinated effort with the objectives of minimizing disruptions of service to the institution and its customers, minimizing financial losses, and ensuring a timely resumption of operations in the event of a disaster.

This chapter is divided into two primary sections. The first section will discuss the responsibilities of an institution's board of directors and senior management in providing contingency planning on an organization-wide basis. The second section will discuss a subset of the organization's plan dealing with the resumption of IS operations following a disruption of processing.

CORPORATE CONTINGENCY PLANNING RESPONSIBILITIES

Corporate contingency planning is a process of reviewing an institution's various departments, business units, or functions and assessing each area's importance for the viability of the organization and providing customer services. Plans are then developed to restore critical areas should they be affected by physical disasters, such as fires or flooding; environmental disasters, such as power failure or telecommunication failure; or, other disasters, such as theft or restricted access to facilities.

The board of directors is responsible for annually reviewing and approving the institution's disaster recovery plans. In addition, the board should be apprised of the scope, frequency and test results of the plan's effectiveness. Senior management is charged with conducting a periodic assessment of the criticality of all business areas, evaluating the area's susceptibility to disasters (including their dependence on continued performance by outside parties), and formulating and testing contingency plans. As stated above, one of the primary objectives in corporate contingency planning is limiting financial losses should a disaster occur. A well researched, current, and comprehensive contingency plan will greatly aid management in selecting reasonable cost solutions in highly stressful disaster situations. (See FFIEC Examination Policy SP-5: "Interagency Policy On Contingency Planning For Financial Institutions.")

ORGANIZATIONAL PLANNING GUIDELINES

At a minimum, the board of directors and/or senior management should:

Obtain commitment from senior management to develop the plan.

Establish a management group to oversee development and implementation of the plan. In larger institutions this may involve a full-time staff to coordinate and track individual business unit plans.

Perform a risk assessment.

- Consider possible threats such as:
  - Natural: fires, flood, earthquakes.
  - Technical: hardware/software failure, power disruption, communications interference, etc.
  - Human: riots, strikes, disgruntled employee, sabotage, etc.
- Assess impacts from loss of information and services from both internal and external sources:
  - Financial condition.
  - Competitive position.
  - Customer confidence.
  - Legal/regulatory requirements.

- Analyze costs to minimize exposures.

- Evaluate critical needs. This evaluation also should consider timeframes in which a specific function becomes critical.

  - Functional operations.
  - Key personnel
  - Information
  - Processing systems
  - Documentation
  - Vital records
  - Policies/procedures

- Establish priorities for recovery based on critical needs.

- Determine strategies to recover.

  - Facilities.
  - Hardware.
  - Software.
  - Communications.
  - Data files.
  - Customer services.
  - User operations.
  - MIS.
  - End-user systems.
  - Other processing operations.

- Obtain written backup agreements/contracts for:

  - Facilities.
  - Hardware.
  - Software.
  - Vendors.
  - Suppliers.
  - Disaster recovery services.
  - Reciprocal agreements.

- Organize and document a written plan.

  - Assign responsibilities to:
    - Management.
    - Personnel.
    - Teams.
    - Vendors.
    - Security.

- Document strategies and procedures to recover.

- Develop procedures to execute the plan's priorities for critical vs. non-critical functions:

  - Site relocation (short-term).
  - Site restoration (long-term).
    - Human.
    - Financial.
    - Technical (hardware/software).
  - Data.
  - Facilities.
  - Administrative.
  - Vendor support.

- 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.

- Present the contingency plan to senior management and the board for review and approval.

- After approval, store a copy of the plan off-site with other reserve supplies.

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.

Reserve supplies should be maintained in appropriate quantities at an off-site location. Management should maintain a current inventory of what is held in the reserve supply.

BACKUP AND CONTINGENCY PLANNING

Disaster recovery planning is a vital to the overall automation security program and the safety and soundness of any institution. The disaster recovery plan should be part of the business resumption plan, which covers every aspect of the bank in the event of an emergency. The ability to efficiently and effectively

recover operations after an emergency reduces the risk of financial loss to the organization and minimizes the level of disruption to the customer.

The disaster recovery plan should not be restricted to traditional mainframe and minicomputer environments. Because of the proliferation of microcomputers and distributed data processing environments (local area networks), critical applications no longer reside only on mainframes or minicomputers. In addition, disaster recovery and contingency planning are not only for large IS operations and facilities, but for institutions with smaller computer systems as well.

The disaster recovery plan should include protection against physical disasters and other disruptions to operations; backup considerations related to hardware, software, applications, documentation, procedures, data files, and telecommunications; and insurance policies regardless of the type of computer equipment and software, and size of the IS facilities within the organization. The contingency plan should be written, approved by the board of directors, and tested annually. This preparation will enhance employee responsiveness, alleviate confusion, and provide for logical decisions during a crisis.

Microcomputer Contingency Planning

The importance of adequate backup resources and procedures for microcomputers cannot be overemphasized. Microcomputer hardware and software technology is ever-changing, and current operations quickly can become outdated. Because of this, contingency planning must begin during the initial acquisition stage and be updated as new hardware and software are acquired.

Protections against equipment failure and data loss should be considered for microcomputers. Because microcomputers are often located outside the protected data processing environment, they are exposed to personnel with insufficient training in their use and exposed to ordinary environmental contaminants. These exposures could cause data loss. The amount and nature of data lost can vary, but an effective backup program, could restore normal operations in an organized and efficient manner.

Basic guidelines for IS backup, contingency planning, and disaster recovery are contained in the following sections. Although these guidelines were developed for larger systems, they also are applicable to microcomputers. This section supplements those guidelines by addressing the risks and exposures specific to the backup of microcomputers and their software and data.

Backup provides continuity of operations. It could be as important in a microcomputer environment as it is in large mainframe centers. Backup standards provide:

- Written backup procedures.
- Maintenance of data file listings, their contents, and locations.
- Hardware, software, and network documentation.
- Minimizing risks involved in the transfer of backup data, whether by electronic link to a mainframe or through the physical transportation of diskettes/tapes to and from the storage site.
- Establishing cross-training programs and levels of responsibility for backup personnel.
- Data integrity, client confidentiality, and the physical security of hardcopy output, media, and hardware.

Depending on the size of the institution and the nature of anticipated risks and exposures, the time spent backing up data is minimal compared with the time and effort that could be necessary to restore it. Files that can be backed up within a short period of time may require days, weeks, or months to recreate from hardcopy records. Therefore, adequate procedures must guide backup operations. They should include:

- Identification of an alternate processing mode, e.g., redundant hardware system located elsewhere; or reciprocal agreement to share compatible hardware with other units within the same institution or in another institution; or backup within the mainframe itself (some institutions enter into agreements with vendors for speedy replacement of software and hardware that has been lost or stolen).

- Off-site storage of software and data.
- Frequency of update and retention cycles of backup software and data.
- Periodic review of software and hardware for compatibility with backup resources.
- Periodic testing of backup for effectiveness in restoring normal operations.
- Guidelines for the labeling, listing, transportation and storage of media.

A coordinator should be assigned to monitor a contingency planning program. Depending on the size of the organization, a user group may be formed to develop and update policies and procedures to assure continued program effectiveness. Further, such a group also could aid the coordinator in implementing and monitoring the program. Membership in this group may include:

- Contingency planning coordinator.
- Microcomputer users at line supervision level.
- Network Administrator.
- Security administrator.
- Internal auditor.

Decisions on application and file backup must be based on how critical the application or files are to the institution's operations. In establishing backup priorities, consideration should be given to all types of information and the potential impact from loss of such data. This includes financial, regulatory, and administrative information, and operating and application software. In assigning backup priority, a risk analysis should be performed that addresses whether:

- The loss of these records would significantly impair the institution's operations.
- The records are being used to manage corporate assets or to make decisions regarding their use.
- Their loss would result in lost revenue.
- Any inaccuracy would result in significant impact on the financial institution, customers, or other departments in the institution.

Frequency of file backup must also depend on the criticality of the application and files. Critical data should be backed up using the "grandfather-father-son" method (see Chapter 13). Backup of operating system software and application programs must be performed whenever they are modified or updated.

Microcomputer software and file backup must not always be kept at an off-site location. Depending on the importance of the information, storage of backup diskettes in another part of the building may be sufficient protection. However, this decision should be based on a risk assessment rather than on ease of access. All backup diskettes should be adequately labeled to identify owner, use, and retention period. The storage location – whether on-site or off-site – should be environmentally controlled and secure, with procedural provisions for restricting physical access to authorized personnel.

IS CONTINGENCY PLANNING

A comprehensive plan should be in place to minimize exposure to all notable threats and risks. This program should emphasize the need for asset protection, security, and controls. The degree of control should be based on an assessment of risk relative to the value of the asset or service. It also should reflect proper concerns for the sensitivity of information. Three major areas that must be reviewed are: physical security; data security; and backup and contingency planning. Physical and data security issues are discussed in Chapter 14. Backup and contingency planning issues will be the focus of this section.

PROTECTION AGAINST PHYSICAL DISASTERS AND OTHER DISRUPTIONS

Physical disasters may be created by man or result from natural phenomena. Regardless of the cause, the best defense against severe loss is effective backup procedures covering equipment, data, operating systems, application software, and documentation.

These provisions enable reconstruction to be accomplished with a nominal amount of confusion and delay. A summary of basic security measures for major physical risks follows.

Fire

Computer center personnel must know what to do in a fire emergency. Instructions should be posted in prominent locations. Fire alarm boxes and emergency power switches should be clearly visible and unobstructed and fire drills should be held periodically. Automatic extinguisher systems include halon, carbon dioxide and water sprinklers. These systems should be the staged type, where the action triggered by a fire detector permits time for operator intervention before it shuts down the power. Computer operations personnel should know how to respond to these automatic extinguishing devices, as well as the location and operation of power and other shut-off valves. Waterproof covers should be located near the equipment in the event that the sprinklers are activated. Hand extinguisher and floor tile pullers should be placed in suitable locations that are easily accessible and vividly marked.

All computer installations should be equipped with heat or smoke detectors. Ideally, these detectors should be located in the ceiling, in exhaust ducts, and under raised flooring. Detectors situated near air conditioning or intake ducts may hinder the build up of smoke to trigger the alarm. The emergency power shutdown should deactivate the air conditioning. Walls, doors, partitions, and floors should be fire-resistant. Also, the building and equipment should be grounded correctly for protection from electrical hazards.

The extent of fire protection required for a data center depends on the degree of risk a financial institution is willing to accept. If the financial institution has major applications on the computer and if appropriate backup facilities are not available, every effort should be made to install the most effective fire extinguishing system. On the other hand, if adequate backup facilities are available or only minor applications, i.e., fixed assets, payroll, securities, are on the system, extensive fire prevention equipment would not be necessary. On-line systems require increased fire protection, since complete backup is more difficult, if not impossible, to obtain.

Flooding

A financial institution should not locate its computer installation in or near a flood plain. If the computer equipment is placed below ground level or a sprinkler system is used, precautions should be taken to limit water damage. If there is a floor above the computer room, the computer room ceiling should be sealed to prevent water seepage.

Sabotage and Riot

Computer center personnel should know how to handle intruders, telephone bomb threats, and other disturbances. Since attacks on computer installations have occurred, their locations should be inconspicuous. Sabotage could be caused by a disgruntled employee. Therefore, personnel policies should require the immediate termination and removal from the premise of any employee considered a threat. Obviously, locked doors, intrusion detection devices, guards, and other controls that restrict physical access are important preventive measures. As for other disasters, procedures should exist to minimize the probability of occurrence and damage, and to effect a full and prompt recovery.

Power Failure

Voltage coming into the computer room is often monitored by a recording voltmeter and regulated to prevent power fluctuations. In the event of power failure, an alternative power source should be provided. Independent power supply units consist of gas or diesel generators or a battery arrangement that provides electricity for a limited period of time to allow an orderly shutdown of the system. Larger or more complex systems commonly utilize a combination of batteries and auxiliary generator(s) to create an Uninteruptable Power Supply (UPS). The UPS unit enables operations to continue in the event of a power failure or surge.

Housekeeping Rules

Smoking, eating, and drinking in the computer room or when using any computer equipment, such as a microcomputer, should be prohibited. In addition, computer rooms should be kept clean and organized as extraneous supplies and clutter could inhibit the flow of operations or access to emergency exits and controls.

Fraud or Theft

Physical measures to safeguard against loss from fraud or theft are comparable to those outlined for sabotage and riot. Exposure is reduced by restricting access to information that may be altered or misappropriated. Since fraud or theft may be perpetrated easily by insiders, personnel policies should be designed to minimize that possibility. The computer center may be held liable for release of sensitive or confidential information pertaining to its customers; therefore, special procedures to safeguard information are warranted.

Equipment Failure

Equipment failure may result in extended processing delays. Performance of preventive maintenance enhances system reliability and should be extended to all supporting equipment, such as temperature and humidity control systems and alarm or detecting devices.

HARDWARE BACKUP

Hardware backup is the first step in contingency planning. All computer installations must make formal arrangements for alternative processing capability in the event their data center or any portion of the work environment becomes disabled. These plans can take several forms and involve the use of another financial institution, data center, or other installation. In addition, hardware manufacturers and software vendors can be helpful in locating an alternate processing site and in some cases will be able to provide backup equipment under emergency conditions. The more common plans are:

- *In-house* – Many financial institutions operating more than one CPU or local area network (LAN) may be able to provide their own backup for certain critical applications. If the processors are in separate geographic locations, capable of processing critical applications, and are fully compatible, there may be no for other backup locations. If the processors are both located in the same building, the financial institution must develop a plan for outside backup in the event of emergencies.

- *Service bureau* – Many independent service bureaus can provide financial institutions with backup for critical applications. These installations may charge an annual retainer fee in addition to the normal cost of actual backup processing. They should be able to accept the financial institution's work on short notice.

- *Reciprocal agreement* – Many financial institutions enter into agreements with other financial institutions or data processing centers to provide equipment backup. This arrangement is usually made on a best efforts basis, whereby financial institution A promises to backup financial institution B as long as financial institution A has time available.

- *Recovery operations center (ROC) or hot-site* – There are basically two types of processing backup locations: one without equipment but with power, air conditioning, etc. (shell or cold-site);and another in which compatible computer equipment has been installed and awaits use (hot-site). The ROC with installed equipment is normally used by non-priority customers on a timeshareing or random basis. These customers have agreed in advance to relinquish their use to that of an ROC member that has suffered a disaster.

Forms of ROCs or hot-sites vary. Some IS installations have established their own alternative site, while others have formed a cooperative or joint venture with nearby servicers. Cost is a major factor. Various companies have recently begun to market memberships in ROCs/hot-sites at reasonable annual fees, often constructing the facility after a predetermined number of members have committed to join. They may be either shells or fully operational sites whose economies are gained by sharing the costs. Generally, administrative assistance and priority planning are determined by the ROC vendor, with the major disadvantage being the substantial fee assessed if the facility is used.

Potential misunderstandings may be avoided if the financial institution signs a formal written agreement with the management of the backup site, which specifically identifies the conditions under which the site may be used. Basic concerns in establishing hardware backup arrangements include whether:

- The backup system is physically compatible with the primary system. Both hardware and software must be physically compatible to the primary system to process the financial institution's applications.

- The backup installation is a reasonable distance away from the primary system. Ideally, the backup installation should be far enough away to be on a different electric power grid or free from the same natural disaster (earthquake, hurricane, etc.), but close enough to be reached quickly.

- The backup installation is working at peak load. It is of little value to have a backup site that is easily accessible, but has little or no available computer time.

- The backup installation will be advised of impending changes which may effect compatibility or the ability to provide backup. Location and availability of compatible hardware must also be considered before switching to a new hardware system.

Written contingency procedures should, at a minimum, address:

- Conditions or situations that necessitate using the backup site.

- Responsibility for making a decision and guidelines as to when it should be made.

- Employee and vendor notification.

- Backup site notification.

- Steps to be followed at the backup site.

- Files, input work, special forms, etc., to be taken to the backup site and means of transportation.

The backup site should be tested at least annually and when equipment is changed to ensure continued compatibility. To the extent practicable, operating procedures at the backup site should be established with a level of security protection comparable to that for the main data center and other IS operations outside it.

If the institution is small, it may be possible to revert to manual processing, but only as a final alternative. Skills necessary to operate a manual system are soon lost after the application is automated. Unless those skills are maintained through periodic testing, manual processing is usually not a viable alternative.

Hardware backup procedures in a distributed data processing environment (local area network) are similar to that of a mainframe. In the event of a major problem or catastrophic breakdown, off-site processing capabilities should be arranged to ensure continual operations. Contingency plans should be arranged with another institution, data processing center, or other facility.

A major difference in on-site backup between a LAN and mainframe is fault tolerance which is the ability of the LAN to continue functioning in the event of a breakdown with no damage to data and with no perceptible change in operation. Fault tolerance in a network environment entails a duplicate piece of hardware that automatically takes over in case a component on the primary LAN fails. Fault tolerance in a mainframe environment may be difficult to accomplish since the costs incurred with acquiring additional mainframe equipment may be extensive.

The most widely used method of fault tolerance is disk mirroring and/or disk duplexing. With disk mirroring, all programs and data are backed up in real time to a secondary disk drive that can take over if the primary disk fails. This would allow the first or primary drive to be replaced without disrupting server operations. Disk duplexing can be synonymous with disk mirroring, but disk duplexing generally utilizes two controller cards versus one. Regardless of the exact interpretation, disk duplexing entails a greater degree of redundancy than mirroring.

PROGRAM AND SOFTWARE BACKUP

In addition to hardware backup, program backup is another important phase of contingency planning. Program backup for all hardware platforms consists of three basic areas: operating system software, application software, and documentation. All software and related documentation must have adequate off-premise storage. Even when using a standard software package from one vendor, the software probably will vary from one location to another. Differences may include interest rate modifications, reporting options, account applications, or other options chosen by the institution during or subsequent to system implementation. The more nonstandard an institution's software, the more critical it becomes to have off-site storage.

The operating system software must be backed up with at least two copies of the current version. Without it, even the most sophisticated computer hardware is useless. One copy should be stored in the tape and disk

library for immediate availability in the event the original is impaired; the other copy should be stored in a secure, off-premise location. Duplicate copies should be tested periodically and recreated whenever there is a change to the original.

Application software, which includes both source and object versions of all application programs, must be maintained in the same manner as the operating system software. Backup copies of the programs must be updated as program changes are made. Minor updates to backup copies can be made on a group basis, but major revisions or enhancements to application programs should be updated immediately. Storing, testing, and updating such software should be addressed in the installation's contingency plan.

Software vendors can usually supply institutions with copies of standard application software products if they are destroyed. However, even assuming that the vendor has accurately maintained the institution's parameter selections and modifications, there will probably be additional expenses and some delay in making the software operational. Under these circumstances, the institution is placing responsibility for storing software with vendors. Most vendors are reluctant to guarantee software availability, because they may not have current sets of the institution's software. This does not apply to software kept by third parties under an escrow agreement (See Chapter 12). Thus, a financial institution should maintain its own software backup at an off-site location to be assured of only a limited interruption in processing during an emergency.

Documentation for the operating system and the application programs also should be backed up. A minimum level of documentation should be maintained at an off-site location. This includes current copies of:

- Operating system options and modifications.
- Application flowcharts.
- Descriptive narrative for all systems and programs.
- File layouts and transaction codes.
- Operator run instructions.
- User manuals.

The requirement for off-site storage of user manuals can be satisfied by distributing these documents to user departments remote to the data center and institution.

Procedure manuals also are necessary during disaster recovery. Duplicate copies of all IS related procedures should be stored at the off-site location. These include manuals on systems and programming standards, documentation, file libraries, computer operations procedures, and data control procedures. Most important, a copy of the procedures outlining plans for IS operations during emergencies should be maintained off-premise.

DATA FILE BACKUP

The most important area of backup involves the institution's data files, regardless of the platform in which the data is located. Financial institutions must always be able to generate a current master file. Data files must be backed up both on-site and off-site to provide a recovery capability. Retention of current data files, or older master files and the transaction files necessary to bring them current, is important so that processing can continue in the event of a disaster. The creation and rotation of data file backups is a daily activity in most institutions.

TELECOMMUNICATIONS BACKUP

A data center must develop an effective backup plan that includes an agreement for alternative site processing. For telecommunications, that plan also must address the communications media and equipment. The contingency plan should establish priorities, i.e., bank tellers versus ATMs, data versus voice lines, particular offices or sites, and transactions processed versus inquiries, and should identify critical components of the network (such as if all lines in the building connect to a Private Branch Exchange (PBX) and the building is serviced by a single cable to the telephone company central office (CO), alternate routes to the backup CO must be identified as well). Rerouting and redundancy may permit the use of alternate equipment, facilities, lines and circuits, but may still be limited by other considerations. Considerations include risk versus economics, the practicality of the selected backup components, and the security and data integrity provided by the backup plan.

Risks may be addressed by assessing the individual components in the network, the dependence on each component, and the probability of it going down or

becoming unavailable or unreliable. A financial institution must analyze the business impact- including cost or lost dollars - regulatory and legal requirements, and customer satisfaction to assess backup costs. The costs of various backup alternatives must be weighed against the extent of risk protection each provides. This assessment also should address costs associated with testing, since all components of a plan should be tested periodically, including the communications media.

A financial institution should have a file identifying all circuits by circuit number and a matrix outlining their location, priorities and uses. A duplicate of this file should be maintained at a different location in case of any problems.

The backup plan must address the practicality of each component. Selected alternatives must be able to accommodate the anticipated volumes or capacities at the necessary speeds to meet the established priorities. For example, several dial-up lines may not be a practical replacement for a T1 line. The backup plan must recognize availability and lead times required to employ certain components, such as installing additional lines or modems and multiplexers at a backup site. Reliability, flexibility, and compatibility – all components of the original planning process – also must be considered in formulating the backup plan. For example, a modem used for backup may not provide the service required, or a line may satisfactorily transmit voice, but be insufficient in quality and speed for data. Additionally, the telecommunications backup plan must be compatible with other contingency plans in the institution, since it will affect users, data processing, and customers.

Security and the data integrity of alternative components used must be considered in the contingency plan. Switching from fiber optics to wire pair, dedicated to switched, or digital to analog may make the line more susceptible to a wire tap or to line noise, which can result in errors. Using dial-up lines could facilitate access by the public. Alternate equipment selected should be checked to determine if it permits encryption.

The relative importance of the applications processed and the extent to which a financial institution depends on its telecommunications system will determine the degree of backup required. Management should make a careful appraisal of its backup requirements, decide on an effective plan, detail the procedures, and test its effectiveness periodically.

INSURANCE

Insurance is commonly used to guard against loss from risks that cannot be completely prevented. Generally, coverage is acquired for risks with little probability of occurring, but with significant potential for financial loss or other disastrous consequences.

CORPORATE CONTINGENCY PLANNING WORKPROGRAM

CHAPTER 10WP

(FILE NAME ON DISK #3= IS-WP#05.WPD)

COMMENTS

This section is intended to determine whether senior management has instituted a current and workable corporate contingency planning process throughout the organization. Management must develop and maintain an effective recovery planning process in the event a disaster or major disruption disables any functional area(s) of the institution or any of the IS supporting infrastructure that service(s) them. An organization-wide focus to recover must be developed for all IS areas from the smallest stand-alone PCs and LANs to centrally located minicomputers or the central mainframe computer center. All IS support activity and the functional customer areas they serve must have a clearly defined and fully integrated recovery plan. The direction for such planning must originate from the senior level and address fully all aspects of the institution's operational activity that supports the delivery of services to both internal and external customers. The examiner should document findings, especially those that do not satisfy the recommendations outlined in the 1996 *FFIEC IS Examination Handbook*. This document will be included in the workpapers.

CORPORATE CONTINGENCY PLANNING

1. Determine if the board has approved an organization-wide contingency plan within the last 12 months.

2. Determine if a senior manager has been assigned responsibility to oversee the development, implementation, and maintenance of the corporate contingency plan.

3. Determine if management periodically reviews and prioritizes each business unit, department, and functional unit for its critical importance. If so, determine how often are reviews conducted.

4. Review the written corporate contingency plan and verify if the plan:

    a. Addresses all the critical business units/departments/functions identified in step 3.

    b. Has a clear and current employee/manager notification tree.

    c. Clearly defines responsibilities and decision-making authorities for designated teams and/or staff members.

    d. Documents guidelines for recovery-related expenses for later insurance or tax-loss claims.

e. Designates a public relations spokesperson.

f. Identifies sources of needed office supplies and equipment.

g. Addresses the recovery of free standing PCs and LANs. If this is not included in the plan, check to see there is a separate plan for recovery of these resources.

5. Determine if adequate procedures are in place to ensure the plan is maintained in a current fashion and updated regularly.

6. Determine if personnel are adequately trained as to their specific responsibilities under the plan.

TESTING

7. Check to see how often is the corporate contingency plan tested.

8. Verify that all critical business units/departments/ functions are included in the testing.

9. Verify that tests include:

   a. Setting goals in advance.

   b. Realistic conditions and activity volumes.

   c. Use of actual backup system and data files from off-site storage

   d. Participation and review by internal audit.

   e. A post-test analysis report and review process that includes a comparison of test results to the original goals.

   f. Development of a corrective action plan for all problems encountered.

10. Determine if interdependent departments have been involved in testing at the same time to uncover potential conflicts.

IS CONTINGENCY PLANNING

11. Determine if the data center has a properly documented contingency plan. Verify that the IS

contingency plan properly supports and reasonably reflects the goals and priorities found in the corporate contingency plan.

12. Review the written IS contingency plan to determine if it:

    a. Clearly identifies the management individual(s) who have authority to declare a disaster.

    b. Clearly defines responsibilities for designated teams or staff members.

    c. Explains actions to be taken in specific emergency situations.

    d. Allows for remote storage of emergency procedures manuals.

    e. Defines the conditions under which the backup site would be used.

    f. Has procedures in place for notifying the backup site.

    g. Has procedures for notifying employees.

    h. Establishes processing priorities to be followed.

    i. Provides for reserve supplies.

13. Determine if all critical resources are covered by the plan, including data communication networks, ATMs, etc.

14. Determine if the plan includes stand alone PCs and LANs. If it does not, check to see if there is a separate plan for those resources.

15. Determine if a copy of the IS contingency plan is stored offsite.

HARDWARE BACKUP

16. Describe arrangements for alternative processing capability in the event the data center or any portion

of the work environment becomes disabled and document that the arrangements are in writing.

17. If the organization is relying on in-house systems in separate physical locations for backup, verify that the equipment is capable of independently processing critical applications.

18. If the organization is relying on outside facilities for backup, determine if the backup site:

    a. Has the ability to processes the required volume.

    b. Provides sufficient processing time for the anticipated workload based on emergency priorities.

    c. Allows the institution to use the facility until it achieves a full recovery from the disaster and resumption of activity at the entity's own facilities.

19. Determine how customers would be accommodated if simultaneous disaster conditions were to occur to several customers of the backup facility provider.

20. Determine whether the institution would be kept informed of any changes at the recovery site (e.g. hardware or software upgrades or modifications) that might require adjustments to the institution's software or to the recovery plan.

21. Determine if the plan provides physical security at the recovery site.

PROGRAM OR SOFTWARE RECOVERY

22. Coordinate with the review of backup tape creation and rotation procedures performed under the operations workprogram and determine if:

    a. Duplicates of the operating system are available both on- and off-site.

    b. Duplicates of the production programs are available both on and off-site. Including both source and object versions.

    c. All programming and system software changes are included in the backup.

d. Backup media is stored off-site from which it can be retrieved quickly at any time.

23. Review the written IS continency plan and determine if the plan addresses the backup of the systems and programming function (if applicable), including:

    a. Qualified personnel.

    b. Backup of programming tools and software.

    c. Off-site copies of program and system documentation.

24. Verify the IS contingency plan provides for logical security procedures at the recovery site.

DATA RECOVERY

25. Coordinate with the review of backup tape creation and rotation procedures performed under the operations workprogram and determine if all master files and transaction files are backed up adequately to facilitate recovery should a disaster occur.

NETWORK RECOVERY

26. Determine if management assesses the network environment including:

    a. The individual components in the network.

    b. The dependence on each component.

    c. The probability of a component going down or becoming unavailable or unreliable.

TESTING

27. Determine if the IS contingency plan is tested at least annually.

28. Determine if all critical applications and services tested.

29. Determine if the tests include:

    a. Setting goals in advance.

    b. Realistic conditions and activity volumes.

c. Use of actual backup system and data files from offsite storage.

d. Participation and review by internal audit.

e. A post-test analysis report and review process that includes a comparison of test results to the original goals.

f. Development of a corrective action plan for all problems encountered.

30. Determine if several user departments have been involved in testing at the same time to uncover potential conflicts.

CONCLUSIONS

31. Review the results of work performed in this section and in sections for planning, auditing , and management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections.

32. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

33. Assign a rating (see Chapter 5 for additional information).

34. Prepare an index of workpapers for this section of the workprogram.

35. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem or high risk areas. Also include, important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the

overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

36. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner	Date

Reviewer's Initials

MIS REVIEW

CHAPTER 11

(FILE NAME ON DISK # 1 = S2C11.WPD)

A management information system (MIS) is a process that provides the information necessary to manage an organization effectively. MIS and the information it generates are generally considered essential components of prudent and reasonable business decisions.

The importance of maintaining a consistent approach to the development, use, and review of MIS systems within the institution must be an ongoing concern of both institution management and examiners. MIS should have a clearly defined framework of guidelines, policies or practices, standards, and procedures for the organization. These should be followed throughout the institution in the development, maintenance, and use of all MIS.

MIS is viewed and used at many levels by management. It should be supportive of the institution's longer-term strategic goals and objectives. To the other extreme, those everyday financial accounting systems also are used to ensure that basic control is maintained over financial record keeping activities.

Financial accounting systems and subsystems are only one type of institutional MIS. Financial accounting systems are an important functional element or part of the total MIS structure. However, they are more narrowly focused on the internal balancing of an institution's books to the general ledger and other financial accounting subsystems. For example, accrual adjustments, reconciling, and correcting entries used to reconcile the financial systems to the general ledger are not always entered immediately into other MIS systems. Accordingly, although MIS and accounting reconcilement totals for related listings and activities should be similar, they may not necessarily balance.

An institution's MIS should be designed to:

- Enhance communication among employees.
- Deliver complex material throughout the institution.
- Provide an objective system for recording and aggregating information.
- Reduce expenses related to labor-intensive manual activities.
- Support the organization's strategic goals and direction.

Because MIS supplies decision makers with facts, it supports and enhances the overall decision making process. MIS also enhances job performance throughout an institution. At the most senior levels, it provides the data and information to help the board and management make strategic decisions. At other levels, MIS provides the means through which the institution's activities are monitored and information is distributed to management, employees, and customers.

Effective MIS should ensure that the appropriate presentation formats and time frames required by operations and senior management are met. MIS can be maintained and developed by either manual or automated systems or a combination of both. It always should be sufficient to meet an institution's unique business goals and objectives. The effective deliveries of an institution's products and services are supported by the MIS. These systems should be accessible and useable at all appropriate levels of the organization.

MIS is a critical component of the institution's overall risk management strategy. MIS supports management's ability to perform such reviews. MIS should be used to recognize, monitor, measure, limit, and manage risks. Risk management involves:

- Policies or practices.
- Operational processes.
- Staff and management.
- Feedback devices.

The most efficient and useable MIS should be both operational and informational. As such, management can use MIS to measure performance, manage resources, and help an institution comply with

regulatory requirements, for example, the managing and reporting of loans to insiders. MIS also can be used by management to provide feedback on the effectiveness of risk controls. Controls are developed to support the proper management of risk through the institution's policies or practices, operational processes, and assignment of duties and responsibilities.

Technology advances have increased the volume of information available to management and the directors for both planning and decision making. Correspondingly, technology also increases the potential for inaccurate reporting and flawed decision making. Because data can be extracted from many financial and transaction systems, appropriate control procedures must be set up to ensure that information is correct and relevant. In addition, since MIS often originates from multiple equipment platforms, including mainframes, minicomputers, and microcomputers, controls must ensure that systems on smaller computers have processing controls that are as well defined and as effective as those commonly found on the traditionally larger mainframe systems.

All institutions must set up a framework of sound fundamental principles that identify risk, establish controls, and provide effective MIS review and monitoring systems throughout the organization. Commonly, an organization may choose to establish and express these sound principles in writing. The Federal Financial Examination Council (FFIEC) fully endorses and supports written principles to enhance effective communications throughout the institution. Management should follow sound fundamental principles and govern the risk in the MIS Review area appropriately . However, if sound principles are not effectively practiced, the examiner may require management to establish written MIS policies to formally communicate risk parameters and controls in this area.

Sound fundamental principles for MIS review include proper internal controls, operating procedures and safeguards, and audit coverage. These principles are explained throughout this chapter.

RISKS ASSOCIATED WITH MIS

Risk reflects the potential, the likelihood, or the expectation of events that could adversely affect earnings or capital. Management uses MIS to help in the assessment of risk within an institution. Management decisions based upon ineffective, inaccurate, or incomplete MIS may increase risk in a number of areas, such as credit quality, liquidity, market/pricing, interest rate, or foreign currency. A flawed MIS causes operational risks and can affect adversely an organization's monitoring of its fiduciary, consumer, fair lending, Bank Secrecy Act, or other compliance-related activities.

Since management requires information to assess and monitor performance at all levels of the organization, MIS risk can extend to all operations. Additionally, poorly programmed or non-secure systems in which data can be manipulated and/or systems requiring ongoing repairs can easily disrupt routine workflow and lead to incorrect decisions or impaired planning.

ASSESSING VULNERABILITY TO MIS RISK

To function effectively as an interacting, interrelated, and interdependent feedback tool for management and staff, MIS must be useable. The five elements of a useable MIS system are: timeliness, accuracy, consistency, completeness, and relevance. The usefulness of MIS is hindered whenever one or more of these elements is compromised.

- *Timeliness* – To simplify prompt decision making, an institution's MIS should be capable of providing and distributing *current* information to appropriate users. Information systems should be designed to expedite reporting information. The system should be able to quickly collect and edit data, summarize results, and be able to adjust and correct errors promptly.

- *Accuracy* – A sound system of automated and manual internal controls must exist throughout all information systems processing activities. Information should receive appropriate editing, balancing, and internal control checks. A comprehensive internal and external audit program should be employed to ensure the adequacy of internal controls.

- *Consistency* – To be reliable, data should beprocessed and compiled consistently and

uniformly. Variations in how data is collected and reported can distort information and trend analysis. In addition, because data collection and reporting processes will change over time, management must establish sound procedures to allow system changes. These procedures should be well defined and documented, communicated clearly to appropriate employees, and include an effective monitoring system.

- *Completeness* – Decision makers need complete and pertinent information in a summarized form. Reports should be designed to eliminate clutter and voluminous detail, thereby avoiding information overload.

- *Relevance* – Information provided to management must be relevant. Information that is inappropriate, unnecessary, or too detailed for effective decision making has little, if any, value. MIS must be relevant to support the management level using it. The relevance and level of detail provided through MIS systems directly correlate to what is needed by the board of directors, executive management, departmental or area mid-level managers, etc. in the performance of their jobs.

ACHIEVING SOUND MIS

The development of sound MIS is not the result of a momentary decision by management. Instead, management should develop and enforce a culture of system ownership. An owner is a system user who knows current customer and constituent needs and has budget authority to fund new projects. Building ownership promotes pride in institution processes and helps ensure accountability.

Although MIS does not necessarily reduce expenses, the development of meaningful systems, and their proper use, will lessen the probability that erroneous decisions will be made because of inaccurate or untimely information. Erroneous decisions invariably misallocate and/or waste resources. This may result in an adverse impact on earnings and/or capital.

MIS which meets the five elements of useability is a critical ingredient to an institution's short- and long-range planning efforts. To achieve sound MIS, the organization's planning process should include consideration of its needs at both the tactical and strategic levels. For example, at a tactical level MIS systems and report output should support the annual operating plan and budgetary processes. They also should be used in support of the long-term strategic MIS and business planning initiatives. Without the development of an effective MIS, it is more difficult for management to measure and monitor the success of new initiatives and the progress of ongoing projects. Two common examples of this would be the management of mergers and acquisitions or the continuing development and the introduction of new products and services.

Management must ensure that MIS systems are developed according to a sound methodology that encompasses:

- Appropriate analysis of system alternatives, approval points as the system is developed or acquired, and task organization.

- Program development and negotiation of contracts with equipment and software vendors.

- Development of user instructions, training, and testing of the system.

- Installation and maintenance of the system.

Management also should consider use of project management techniques to monitor progress as the MIS system is being developed. Internal controls must be woven into the processes and periodically reviewed by auditors.

Management also should ensure that managers and staff receive initial and ongoing MIS training. In addition, user manuals should be available and provide:

- A brief description of the application or system.

- Input instructions, including collection points and times to send updated information.

- Balancing and reconciliation procedures.

- A complete listing of output reports, including samples.

Depending on the size and complexity of its MIS

system, an institution may need to use different manuals for different users, such as first-level users, unit managers, and programmers.

MIS REVIEWS

By its very nature, management information is designed to meet the unique needs of individual institutions. As a result, MIS requirements will vary depending on the size and complexity of the operations. For example, systems suitable for community-sized institutions will not necessarily be adequate for larger ones. However, basic information needs or requirements are similar in all financial institutions regardless of size. The complexity of the operations and/or activities, together with institution size, point to the need for MIS of varying degrees of complexity to support the decision-making processes. Examiners should base MIS reviews on an evaluation of whether the system(s) provides management and directors with the information necessary to guide operations, support timely decision making, and help management monitor progress toward reaching institutional goals and objectives. Although examiners should encourage management to develop sound information systems, they also should have reasonable expectations about what constitutes suitable MIS.

MIS reviews are normally focused on a specific area of activity, on a clearly identifiable departmental or functional basis, or as a part of the activity being examined within a larger department.

During the examination, the MIS review should occur at both a macro (big picture) level and a micro (functional/product oriented view of the business) level. The examiner-in-charge of the MIS review program should look at the useability and effectiveness of the corporate-wide MIS structure. The examiner also should collect MIS related observations and information from the examiners-in-charge of the other areas under review. It would be difficult for one examiner to attempt to perform a detailed MIS review for all of an organization's functional and operational areas of activity. It is practical and reasonable, however, for this lead examiner to coordinate and consolidate the MIS reviews from the other examination areas. The MIS related feedback received from other area examiners provides important and practical input to the MIS review examiner. The consolidation, coordination, and analysis of this MIS feedback can be used to reach supportable macro-level conclusions and recommendations for corporate-wide MIS activities.

MIS reviews in the functional or product review areas should generally be performed by an examiner who is considered to be a subject matter expert (SME) in the area of activities or operations supported by the MIS systems or processes under review. The SME must have a thorough and complete understanding of the baseline business supported by the MIS system(s) under review. A solid understanding of the business is fundamental to complete a meaningful MIS review. The decision about the overall quality and effectiveness of MIS generally should be made by the SME for the area under review. The SME for each area where MIS is under review must subsequently communicate MIS related findings, conclusions, and opinions to the examiner charged with the responsibility for the complete MIS Review workprogram at that examination. This is clearly a collaborative effort among area SMEs and the examiner charged with the responsibility for this area of review.

The examiner coordinating the overall MIS review program should be a safety and soundness examiner with broad experience and understanding that covers many areas of organizational operations and activity. Alternatively, an information systems (IS) examiner could serve in this capacity. IS examiners should be consulted whenever there are questions, issues or concerns surrounding the use of Information Systems (IS) technology or the effectiveness of MIS-related internal controls in any automated area of the organization's activities.

When performing MIS reviews, examiners should use the guidelines in this chapter to determine if management has:

- Identified the institution’s specific information requirements. Examiners can focus on specific information needs related to issues, such as asset quality, interest rate risk, regulatory reporting, and compliance. If possible, the MIS review should be concurrent with examinations of the safety and soundness, consumer, fiduciary, and IS activities. This would enhance interaction and communication among examiners.

- Established effective reporting mechanisms to guide decisions. This process includes reviewing controls that ensure that information is reliable, timely, accurate, and confidential.

MIS REVIEW WORKPROGRAM

CHAPTER 11WP

(FILE NAME ON DISK #3 = IS-WP#06.WPD) ***COMMENTS***

This section is intended to evaluate the timeliness, accuracy, consistency, completeness, and relevance of, MIS from the management and user department perspective. The complexity of this MIS review depends upon the extent to which management relies upon MIS. The examiner should document any findings, especially those which do not satisfy the recommendations outlined in the *1996 FFIEC IS Examination Handbook.*

Tier I

SCOPING

1. Review previous MIS review-related examination findings. Review management's response to those findings and:

   a. Discuss with examiners their perception of both the usefulness and applicability of the five MIS elements applicable to MIS systems that have been reviewed or are pending review.

   b. Request copies of any reports that discuss either MIS deficiencies or strengths from the Subject Matter Expert (SME) examiners.

   c. Determine the significance of deficiencies and set priorities for follow-up investigations.

2. Request and review copies of recent reports prepared by internal or external auditors of targeted MIS area(s) and determine:

   a. The significance of MIS problems disclosed.

   b. Recommendations provided for resolving MIS deficiencies.

   c. Management's responses and whether corrective actions have been initiated and/or completed.

   d. Audit follow-up activities.

3. Review MIS-related policies, practices, and processes. Pay special attention to any changes since the previous review.

4. Review reports for the MIS target area(s). Determine any material changes involving the

usefulness of information and the five MIS elements of:

a. Timeliness.
b. Accuracy.
c. Consistency.
d. Completeness.
e. Relevance.

5. Together with the EIC, identify each of the functional or product-related areas to be reviewed at this examination. Once the scope of the MIS review has been determined:

   a. Provide copies of the MIS objectives and examination procedures to the SME examiner(s). Highlight those areas of MIS review that must be addressed during the review.

   b. The MIS review examiner will aggregate these observations, conclusions, and recommendations for each of the functional areas addressed and incorporate them (as appropriate) into the final MIS review conclusions.

   c. If there are issues, observations, conclusions or recommendations related to operational or technology aspects of the institution's MIS, the safety and soundness examiner should coordinate these with an experienced IS examiner.

MIS POLICY AND PRACTICE

6. Review minutes of the board of directors or committee(s) representing the MIS target area(s) for a relevant time period and:

   a. Determine any areas where the packet of information does not seem to meet the five required elements of MIS.

   b. Identify MIS issues for follow up.

7. Select and review samples of ongoing executive reports for the targeted MIS area(s). Determine whether:

   a. The source of the information collected originates from the expected business area.

b. Users of the information are the appropriate employees or managers within that area of activity.

c. The reports are distributed ultimately to the appropriate users.

d. The flow of these MIS information/reports is consistent with the responsibilities reflected on the area's official organization chart.

8. Determine the degree to which management and the staff in an area under review use MIS adequately and can support that its use is appropriate and effective. Perform the following steps:

   a. Discussing the five MIS elements with a senior manager(s) of the respective business unit.

   b. Repeating this step with an employee of the business unit who has experience with the MIS system. (Note: This task is designed to determine if significant differences about the adequacy of the MIS exist among management and/or staff.)

   c. Based on management's self assessment of the useability of its MIS, identifying any planned activities to enhance, modify, or expand these systems.

9. Determine if authorized processes are followed as data is acquired, merged, manipulated, and up-loaded from subsystems.

10. Determine whether established procedures are sufficient to ensure the proper testing of system developments, enhancements, or parameter changes.

11. Review whether final versions MIS software enhancements or parameter changes are installed in a controlled environment that promotes integrity of information.

USER TRAINING AND INSTRUCTIONS

12. Select a system and request copies of relevant user instructions. Determine whether the guidelines are meaningful, easy to understand, and current.

COMMUNICATION

13. Review the lines of communication within the institution and determine the effectiveness of MIS in the following areas:

    a. Communication paths linking executives, appropriate users, and information systems employees.

    b. The flow of communication throughout the organization.

MERGERS AND ACQUISITIONS

14. Determine if the organization has had recent merger and/or acquisition activity. If it has, determine how management at the senior and departmental levels ensure that the resulting MIS supports and includes the five MIS elements mentioned previously. If mergers and acquisitions are frequent, determine whether:

    a. Appropriate policies or practices and procedures have been developed to support such activity from an integrated MIS perspective.

    b. The consolidation of MIS systems in a merger still meets the requirements of a quality MIS system.

AUDIT

15. Has the MIS target area(s) been internally or externally audited in the past two years?

    a. If it has, review the scope of the audit, the findings and management's response(s) to that report.

    b. If it hasn't, coordinate with the MIS EIC in interviewing audit management to determine what their plans regarding an audit review of the MIS system are.

CONCLUSIONS

16. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Auditing, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

17. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

18. Assign rating (see Chapter 5 for additional information).

19. Prepare an index of workpapers for this section of the workprogram.

20. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations

21. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner	**Date**

Reviewer's Initials

Tier II

MIS POLICY OR PRACTICE

1. Does management's MIS policies and/or practices address the following areas?

   a. The definition, purpose, and fundamental components of MIS?

   b. How to achieve effective two-way communication between management and employees and specific avenues to maintain such communication?

   c. Procedures for acquiring, merging, manipulating, and unloading data to other systems?

   d. Guidance for delineating the need for internal/external audit coverage and testing?

2. Is the policy or practice reviewed and updated regularly?

3. Is the policy or practice distributed to appropriate employees?

4. Does the policy or practice regarding MIS development incorporate or require:

   a. Processes for initiating, developing, and completing MIS enhancements?

   b. User approval for each development phase?

   c. Installation of MIS enhancements in a controlled change environment?

   d. Employees to follow policy or practice and processes as data is acquired, merged, manipulated, and up-loaded to other systems?

   e. Employees to be sufficiently trained for new systems and subsequent enhancements?

5. Obtain from the user manuals or the appropriate manager a workflow showing data from the point-

of-entry, through user processes, to the final product. This task is designed to review how information is identified, gathered, merged, manipulated, and presented and: (Depending on the organization's sophistication and system size, examiners may have to develop this workflow themselves.)

a. Discuss the area's MIS process with a representative sample of users and determine if they know where the data is coming from, where it is going, and how it gets there. A complete understanding would suggest the interviewees both use and understand the MIS system(s) supporting them.

b. Identify and note the points where adjustments to data occur.

c. Identify the department staff responsible for MIS-related input data and reports; i.e., obtain a list of users, ad hoc software report writers, and the programmers involved. Compare this information with the material acquired in the immediately preceding item.

d. Determine if preparation and reconciliation processes are sufficient to reasonably ensure integrity of information.

e. Determine if data adjustments are documented adequately.

f. Determine the effectiveness of ad hoc report writing capabilities by reviewing the software vendor's user manual for data presentations.

g. Through observation and interview, determine useability, commonality, simplicity, and effectiveness of MIS reports supporting the decision making process for that area of activity.

MIS DEVELOPMENT

6. Does the internal planning process consider and incorporate the importance of MIS at both the strategic and tactical level and:

   a. Are longer-term strategic goals (beyond two years) supported by the development of appropriate MIS?

b. Are shorter term tactical goals over the immediate 1 or 2 year period regularly and appropriately reviewed and monitored by management?

7. Do project objectives address reported MIS weaknesses and meet business unit requirements?

8. Does management have a process for monitoring project schedules?

9. Does management use a project management technique to monitor MIS development schedules?

10. Does the organization use a consistent and standardized approach or a structured methodology for developing MIS projects?

11. Does the methodology encompass the:

a. Analysis of the concept, organization of tasks, completions of phases and approvals?

b. Development of the program and contracting for equipment and software?

c. Development of user manuals and testing of the system?

d. Post-review of the system and future maintenance of it?

USER TRAINING AND INSTRUCTIONS

12. Determine whether user manuals provide adequate guidelines in the following areas:

a. Complete description of the system.

b. Input instructions, including collection points and times to send updated information.

c. Balancing/reconciliation instructions.

d. Full listing of output reports, including sample formats.

13. Determine the adequacy of MIS training, including whether:

a. Training needs are properly identified and prioritized.

b. Training is organized in a formal classroom setting, is on-the-job, or is a combination of both approaches.

c. Training manuals or other material besides the user manual exist.

d. The training material adequately covers relevant and current issues.

e. Training material is distributed to the appropriate employees.

14. Proceed to procedure 16, Tier I.

Examiner	**Date**
_____	_____

Reviewer's Initials

SYSTEMS DEVELOPMENT AND PROGRAMMING

CHAPTER 12

(FILE NAME ON DISK # 1 = S2C12.WPD)

All information systems processing functions within a systems development or maintenance process should be guided by written standards and procedures. The standards should address systems design, programming, testing, systems implementation, documentation, and software maintenance. They should include guidelines for effective project controls and procedures for reviewing and acquiring software systems. Standards provide a means of determining if the installation is meeting established policy. By defining uniform methods for performing routine tasks, the standards manual can affect profits and efficiency favorably. When used as a training tool, it enables new employees to become productive in a shorter period of time. Systems and programming standards must identify control procedures to ensure program integrity, restrict unauthorized access, and provide adequate systems documentation. The procedures should identify physical restrictions, software controls, and accounting controls required to maintain security within the application systems, operating systems, and data files. The content and format of the standards and procedures manual will vary with the size of the installation. Larger installations may have a multi-volume manual, where each volume addresses a single topic, such as system design, programming, documentation, and operations. Smaller data centers may cover these areas in a single manual. All installations should establish basic written operating standards. The coordination of these standards into an orderly document improves overall organization and control.

Documentation is a record of procedures for performing information systems processing tasks. It is an accounting of both the essential elements of the information systems application and the logic of the computer software programs. Documentation is the basic source of information for those who audit, correct, improve, manage, operate, or use the system. Program documentation is one of the most vital and neglected areas of information systems. It requires input from persons who have insight, the ability to think logically, and an adequate knowledge of programming languages. Management must participate actively in developing appropriate standards for documentation. To a large extent, the achievement of documentation objectives is directly related to the willingness of senior management to establish the necessary standards.

The relatively recent concept of computer aided software engineering (CASE) automates the process of developing and maintaining software.

PROJECT CONTROL

A key factor in a well-managed information systems facility is the process used to control projects for systems and applications development, acquisition, or revision. Often the difference between a successful project and a problem one is the effectiveness of project control. Project management, however, is not a substitute for technical skills.

Systems development must be monitored closely to control costs and ensure the creation of well structured applications. In a relatively small facility, a formal project control system may not be required. If management frequently meets with systems development personnel and uses adequate management techniques, it can effectively control projects. However, a more formal approach to project control is often preferred, and necessary, in many facilities.

A project control system should employ well-defined and proven techniques for managing projects and generating application development records. Each development task should be identified and tracked to determine its status. Tasks are commonly grouped into major development phases to identify significant project milestones. Although formal project control systems differ significantly, they should at a minimum contain:

- Target completion dates for each task or phase of systems development. A final project completion date is determined by carefully assessing all tasks to be performed. Identification of target dates for tasks or phases provides the substance of project control. The status of the project can be determined by comparing actual completion dates

for parts of the project against planned targets. Project status reports should be used to present such comparisons for managerial review.

- Measurement of progress against original target dates. Project monitoring loses significance when original target dates are revised continually. Although it may be necessary to revise target dates, progress should be measured against original targets to better assess time and cost overruns. If development cost overruns become substantial, the justification for the project may need to be reexamined.

- Project control data aids in managing the system and programming function. Such data is appropriate for periodic reports to senior management on project priorities, project status, resource allocations, target deviations, and budgets. Examples of such project planning tools include Critical Path Method (CPM), (PERT) Program Evaluation and Review Technique, and Gantt charts.

SYSTEMS DEVELOPMENT STANDARDS

Development of computer application systems involves many activities. Standards and procedures should govern each activity. Standards should be written for:

- *System design* – To guide the creation of effective, efficient, and control-oriented application systems.

- *Software analysis and selection* – To ensure the acquisition of quality software that meets the institution's need.

- *Programming* – To ensure that desired features and controls are included in application programs.

- *Testing* – To confirm that all programs and systems are tested adequately. Tests should encompass all conceivable data quality or processing problems.

- *Implementation* – To ensure that a newly developed system is complete, that it functions as specified, and that personnel responsible for its operation (user and computer operations) are adequately trained.

- *Cataloging* – To control additions and changes to the production program library to ensure their integrity.

- *Modifications* – To guard against unauthorized software changes.

- *Documentation* – To assess the effectiveness of written material supporting the systems developed or programs changed.

These standards can be used to guide and monitor the activities of systems analysts and application programmers.

Systems Development Life Cycle

A common approach to the management of application software is the process known as a Systems Development Life Cycle (SDLC) also some times called Waterfall System Development. 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 more 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 ensure the integrity of the system. Testing of various stages within large scale integrated systems may require innovative techniques. Reference SP-4.

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.

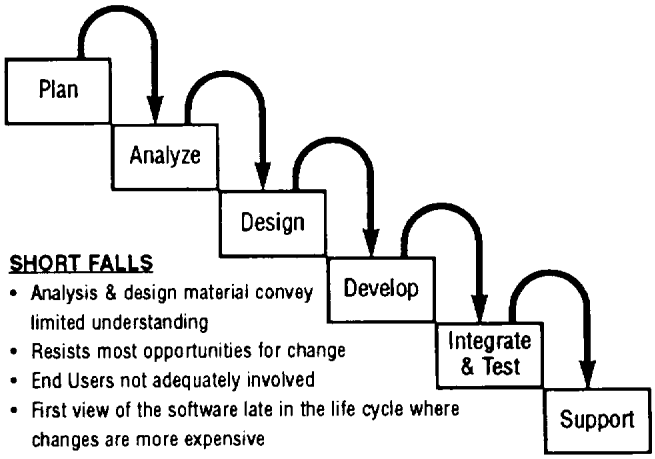
Nevertheless, management must provide more comprehensive employee training since the adoption of a LSIS will affect all departments.

SDLC standards need to be flexible, while still providing maintenance of system integrity during development to maintain that a system of internal control. The SDLC identifies the sequence of activities required in the systems development process and throughout the useful life of an application.

These elements are important to any well-defined systems development process. Each application system has a life cycle, based on a specific series of

functions. The cycle is completed as replacement systems are implemented. Standards should be established and approved for each phase of the development process. Use of a corporate SDLC helps to better plan, implement, and maintain software systems. The following is a brief overview of the major components of an SDLC (Figure 12-1).

Figure 12.1
Waterfall System Development



Project Initiation – Plan

The initial phase of the systems development process addresses conceptual changes and determines the feasibility of pursuing further development. A feasibility study should be performed to identify the expected costs and benefits of developing a specific system. Alternatives to internal application development, such as purchasing software or developing a nonautomated system, should be considered in preliminary evaluations.

Requirements Definition – Analysis

Once a project has been evaluated and approved for development, system analysis and design (involving a variety of complex tasks) proceeds. The requirements definition converts the system concepts into detailed specifications. The analysis and specifications must clearly identify user needs and expectations within the proposed application. This will facilitate development during the design and programming phases and should assist in evaluating vendor software products.

System Design, Development, Test, and Support

Systems design involves the conversion of user requirements into specifications for programming and implementation. The involvement of users is crucial for ensuring that the application design meets their requirements. Systems design techniques vary greatly. However, they should detail the sequence of program flow, the files to be used, the reports to be produced, and the controls to be built into the system. These standards also should identify the content for design documents and the procedures for review and approval. Design documents should include:

- A system narrative identifying the objectives and major functions to be performed.
- A system flowchart identifying the programs, data files, and reports.
- Record layouts showing the content for each data record and file in the system.
- Data element definitions describing each data field.
- Report layouts detailing the format and content for each report produced.
- Screen formats showing the fixed fields and those that are user-modified, including applied edit and control functions.
- Program specification for each program detailing program objectives, files required, and edit routines.
- A test plan validating that programs function properly and produce the expected results.
- A project schedule establishing expected benchmarks for various systems development phases.

The detailed system design can be considered the most important phase of an SDLC. It should represent the approved plan or contract between the user and systems development management.

SOFTWARE ACQUISITION

Many information systems applications for financial

institutions have been developed by software firms. Financial institutions of all sizes find that purchasing software is a cost-effective alternative to developing software systems in-house. Volume sales allow software vendors to provide powerful and flexible products at competitive prices.

Vendors also can provide the necessary technical expertise for continued product support. However, software purchases should be analyzed carefully before any commitment is made. Written standards should exist for evaluating vendor software and for guiding the selection process. Since several vendors should be assessed, a request for proposal (RFP) is generally used to analyze a vendor's capability to meet the needs of the financial institution. An analysis of software products should consider:

- *System requirements* – The institution should identify user needs and expectations for the new system.

- *Systems specifications* – Input/output requirements, interfaces to other systems, and possible future enhancements should be defined.

- *Impact analysis/capacity planning* – The impact that the software will have on existing systems and hardware capacity should be evaluated.

- *A cost/benefit analysis of alternative purchase* – The capabilities of alternative software packages should be evaluated to determine how the proposed system specifications can best be met. A final decision should be reached only after alternative packages are considered.

- *Software support* – The institution must identify responsibility for software support. Many vendors offer software support and maintenance as part of their application system package. Vendors have varying system development processes and techniques which can be a factor in case of maintenance. When contracting for this service, the financial institution must assess both the technical and financial capabilities of the vendor.

If the system is to be supported in-house, the institution must assess its own technical resources and identify:

- *Financial condition of the vendor*s – A vendor should have the financial stability to continue in business and support its products as contracted. The institution should continue to monitor the financial condition throughout the contract term. If financial stability is in doubt, alternatives must be developed to reduce any adverse impact from a loss of vendor service.

- *A well documented system* – A vendor should provide sufficient documentation to allow the user to understand how the software works and the techniques and methods the software uses. This is especially important if program changes are to be performed by the purchasing institution. The format and content of this documentation probably will not be written according to the financial institution's information systems standards. The documentation of program packages under consideration must be reviewed prior to purchase to determine if the product generally meets the financial institution's minimum documentation standards.

  All changes made to application programs and operating systems must be documented according to prescribed standards. The financial institution must have staff with sufficient technical expertise to maintain the software and the documentation. Some vendors provide documentation on magnetic media and this information may be loaded into the on-line documentation system for reference purposes. A potential problem in documentation can arise if the purchased package requires modification before it is installed. It must be determined up front who will modify the documentation with the vendor and/or the purchasing institution involved in the process.

- *Escrow agreements* – Many vendors do not release the source code to the purchaser. This is intended to protect their system's integrity and copyright. The application system is installed in object code. An alternative to receiving the source programs is to establish an escrow agreement. In this agreement, which should either be part of the service contract or exist as a separate document, the financial institution would be allowed to access source programs under certain conditions, such as discontinued product support or financial insolvency by the vendor. Adequate programming and system documentation also should be required. A third party would retain these programs and documents in escrow. Financial institutions should determine periodically that the source code maintained in escrow is up-to-date. This can be done by a third party independently verifying the version number

of the software.

- *Training* – The financial institution's personnel training requirements should be clearly recognized. Training should cover such functions as system operations, problem resolution, input/output controls, file backup, and system support. Vendor responsibility for training should be stated in writing and clearly understood by both parties.

Regardless of whether purchased or developed in-house, the cost of software should be amortized over a reasonable period of time recommended by the institution's accountants.

PROGRAMMING STANDARDS

Although creativity in programming is both necessary and desirable, certain standards are needed to control the development of efficient software. A variety of programming techniques may be employed for this purpose. Standards should establish controls and procedures that must be followed during the programming phase. Although it is not possible to dictate the use of a specific technique in a certain program, all programs should contain some of the following controls:

- Accumulating detailed data and proving them to established control totals. Debit/credit totals, batch totals, and item counts are examples of this type of program control.

- Verifying data input in initial program editing. This allows corrections before erroneous data generates invalid results. This is possible for most applications.

- Using file labels for tapes and disk files to identify specific files, creation dates, and other information that establishes unique identity. This technique guards against invalid processing caused by computer operators selecting and mounting incorrect data files. To be effective, this control must be accompanied by an operational procedure that restricts the operator's authority to override programmed file label checks.

- Embedding edit routines in program code to verify specific data fields. Some examples are:

  - Sequence checks that verify that an item is in proper order for processing.

  - Overflow checks that prevent a data item from entering a storage field too small to accept it.

  - Format checks that verify that data in certain areas are in proper mode (numeric, alphabetic, or alphanumeric).

  - Reasonableness checks that compare data against known factors about the data items or classes of data.

  - Completeness checks that test to see if entries appear in fields that cannot be processed blank.

  - Range checks that compare a data item against set parameters.

  - Check digits that are generated as mathematical functions of the remainder of the field i.e., they permit program computation of the validity of data in input fields.

  - Data items that can be compared in different files or matched against prior period data items to determine reasonableness.

Many types of data integrity checks exist. They are useful in controlling data errors and should be included in applications programs. Program documentation should include a listing of all controls. Such controls include:

- *Restart capability* – Typically, specific stages of processing are identified. Checkpoints are established between processing stages and restart points. Data processed before a restart point is saved. Processing can be resumed at the checkpoint rather than starting from the beginning.

- *Transaction logging* – For on-line applications, the logging of all transactions processed or reflected by input programs provides a complete audit trail of actual and attempted entries. The log can be stored on tape or disk files for subsequent analysis.

- *Standardized program routines* – Many standard routines can be devised and merely embedded in applicable programs to avoid programming duplication.

- *Exception reporting* – Parameters are included in programs to identify unusual or nonstandard transactions. These uncommon transactions should be

captured and recorded on exception reports for subsequent analysis. Exception reporting is a common method of control.

TESTING STANDARDS

As in the design phase, testing is an important phase of the programming process. Here the design and overall reliability of the application system is proven. Tests should be conducted using predetermined data under controlled conditions. This ensures that data will be processed correctly, and reliable output will be produced in the desired format. Strict standards should be developed to govern the testing process. Standard testing procedures should require:

- *A documented test plan* – This identifies specific files, data fields, calculations, and processing routines to be tested. It also should state the test periods e.g., daily and end-of-month.

- *A parallel test of new application systems* – This output can be compared with that existing to determine processing validity.

- *Independent verification of test results by user representatives* – Often users will assume complete responsibility for preparing test data and conducting tests. This is commonly referred to as user acceptance testing. Final test results should be reviewed by all affected parties, including computer operations personnel.

- *A restriction against the use of live files in testing to prevent destruction or alteration of live data* – A copy of a live file can be made to use for testing. Stress/volume tests should be included to ensure that the system can function at peak periods of transactions.

- *The simulation in test data of all possible error conditions to ensure that the program effectively handles all situations* – Although it is difficult to anticipate every error condition, test standards should specify that all abnormal processing conditions be tested. Inadequate testing is often responsible for processing errors that materialize months after the application system becomes operational. Test data generators (software) can aid in developing complete test data.

- *A thorough test of any changes to existing programs may include regression testing (testing of unchanged code)* – Often a simple program change can trigger a malfunction in an apparently unrelated area of a program or system. Ideally, a complete test of all program conditions should be performed each time a logic change is made. Program changes made in haste are often responsible for processing malfunctions and unwanted expenditures of programmer time in researching problems. Also, if copies of live files are used for testing, precautions should be taken to avoid any mix-up between test results and regular output reports.

SYSTEM IMPLEMENTATION

An institution should have written standards for implementing software changes and new systems to ensure that they are ready for production. Implementation standards should require:

- Documented acceptance of the application system by users and computer operations department. This verifies that the programs have been tested thoroughly and are ready for production.

- Complete user and operator run manuals describing each of the processing steps. Manuals must be employed in application testing to identify confusing or invalid operational instructions. The quality and reliability of such manuals is vital to successful information systems operations.

- System training for all users and computer operators. They should be specifically prepared to handle all known abnormal processing and data error conditions. Training should focus on following written procedures.

- Complete documentation before implementation. Analysts and programmers often tend to delay completion of documentation in favor of beginning the next project. Although documentation is generated during the design phase, it must be completed before this phase.

System Evaluation

A post-implementation review should be conducted shortly after the application has begun to operate. The review is conducted primarily to assess the operational performance of the application beyond an initial shakedown period. All parties actively involved with its operation should be interviewed and specific problems noted. Additionally, the relative

success of the project should be gauged by comparing planned and actual costs, benefits, and development time. The results of the review should be documented in a post-implementation evaluation report presented to management. Post-implementation reviews should include:

- *Planned development time and cost compared to actual time and cost* – Management should be aware of projects that dramatically exceed planned cost and time targets. Future project selection and planning should be based on past experience.

- *Design objectives* – It should be determined that the application functions according to design specifications.

- *Potential savings (if applicable)* – Actual cost savings over a controlled period should be compared to the original estimated savings for a similar period. If the planned benefits do not materialize, reasons should be reviewed.

- *Identification of operational problems* – After the application has been in use, operational problems not identified during testing are likely to appear. The post-implementation review can identify problems and suggest future improvements. These secondary modifications are often important in perfecting the system.

- *Non-monetary benefits* – Planned and actual benefits should be compared to assess the project's success.

SOFTWARE MAINTENANCE

Some modification of information systems programs will be necessary during the application life cycle. Changes may be required by program problems, variance in internal operations, competitive demands, or other factors, such as regulatory changes. Whatever the justification, program changes must be strictly controlled and documented to prevent fraudulent or inadvertent modification.

Program Change Control

Requests for program changes should be documented on a standard change request form. The form is used to describe the request and document the review and approval process. It should contain:

- Date of the change request.
- A control sequence number.
- Program or system identification.
- Reason for the change.
- Description of the requested change.
- Person requesting the change.
- Benefits contemplated from the change.
- Projected cost.
- Signed approval authorizing the change, including, at a minimum, the user, appropriate level of information systems personnel, and audit (at least for significant changes).
- Name of programmer assigned to make the change.
- Anticipated completion date.
- User and information systems approval of the completed program change.
- Implementation procedures (steps for getting the program into the production library).
- Implementation date.
- Audit review of change (if deemed necessary).
- Documented sign-off.

Request forms can be pre-numbered or assigned a control sequence number as they are used. They might be filed numerically or by application. However maintained, the request forms should provide an accurate chronological record of the description of all changes to production programs. These records enable:

- The user to track all requested changes accurately.
- Information systems management to monitor the number and status of changes and allocate them to proper cost centers.
- The audit department to review significant changes for authorization and conformance to established standards.

Copies of the program change forms ordinarily should be distributed to the requestor, the system

user, and the programming unit. Depending on the internal control process, the audit department may either require a copy or have access to copies. Notification of program changes to the audit department should not constitute or replace an audit of the program change process.

Both the user and programming management should review and approve change requests. This allows each unit to be aware of pending changes and clarify the specific request. Requested changes should be screened before acceptance to determine alternate methods of making the changes, the cost of the changes, and time requirements for programming. A risk analysis model also could be applied.

Strict procedures should be established to control the movement of modified programs into the production environment. These procedures should identify:

- The security of the programs before production.
- The approval process required to promote programs to production.
- The personnel responsible for placing the programs into production.

Once program modifications have been completed, all program codes (load module, object code, source code, patch code, etc.) should be secured. This will provide some assurance that any program cataloged to the production environment is an unaltered version of the tested and approved program.

The program approval process should include verification of test results, inspection of the code, and verification that the source code and the object code match. Verification of test results should be done according to testing standards.

A list of modified programs should be compared to the authorized change documents to determine that only approved changes were implemented.

Programming personnel should not be responsible for moving programs into production libraries. This responsibility should be assigned to an independent quality assurance/production control function in larger financial institutions or to supervisory operations personnel in smaller ones.

Systems programmers must modify operating systems periodically to resolve operating problems or implement enhancements. Control procedures for modification of operating systems should parallel those for changes to application programs. This includes prior author-ization, documentation, and review of the change. The absence of sound controls and documentation can cause problems when new releases of operating systems are installed.

All program changes should be fully documented. The approved program change request form usually can provide most of the needed documentation. Revisions to program documentation should occur when a change is implemented.

Temporary Program Changes

Occasionally, the need for a program change arises that must bypass the normal change procedures. Such a change might be required to restore production processing. These immediate changes are usually called patches, program temporary fixes (PTF), or temporary program changes (TPC). Sometimes the program object code is changed directly. In other cases, temporary changes to the source code can be made in a separate version of the program. The use of such techniques should be strictly controlled to prevent unauthorized changes and to ensure that approved changes are made correctly. The following controls should be adhered to:

- All temporary changes should be approved in advance by supervisory personnel.
- If the source code is changed, altered instructions should be reviewed by a knowledgeable supervisor.
- A form should be used to document temporary changes, although it often cannot be completed until after the change is made. The form should identify the change, indicate the reason for the change, detail the instructions altered, identify who made the change, the date it was made, and provide a signature of authorization.
- After a temporary change is made, the normal program change procedure should be completed as soon as possible. In the event a patch or PTF is made, the source code must be altered and recompiled to replace the patched object code.

INTEGRATED SOFTWARE SYSTEMS

Application software that combines multiple banking applications and processing functions is known as integrated software. Many financial institutions are converting to integrated systems to meet competitive demands, improve timeliness of information, foster operational efficiency, track the cross-selling of available services, and ease the introduction of new products.

Conventional software applications, such as demand deposits and installment loans, are designed to operate as separate systems. Each application has its own master files, transaction files, and unique program logic. Usually, there is little or no shared data between applications. In addition, programs that provide processing instructions for common functions, such as calculations, accounting, record structuring, or printing are unique to each application.

To improve the efficiency of applications systems, integrated systems were developed. In more basic system designs, integrated software is used to link separate applications. In these systems, data common to each application is stored and accessed through a customer information file (CIF, may also be called a central information file). The records might include customer(s) name, address, account number, and balance. Some of the data is maintained directly in this CIF system. Other data is transferred daily from the processing applications to the CIF. By consolidating this data from separate applications, all customer relationships with the institution can be accessed quickly. This improves operations, increases controls, and allows better customer service. This design has been particularly beneficial to tellers, customer service representatives, and managers. This CIF concept differs from a data base management system (DBMS), since the files are still sequentially accessed. Another differentiation between CIF and DBMS is that CIF tells you the name and address of accounts, while DBMS stores the actual data.

Large Scale Integrated Systems

Certain fully integrated systems combine multiple applications into a single processing system. These large scale integrated systems (LSIS) require a complex design. The system architecture may be horizontal or vertical. Under a horizontal structure, applications such as deposits, loans, and general ledger are linked. Under a vertical structure, functions are linked. For example, a teller transaction is processed at the teller station, additional transactions and entries are generated for operating departments affected by that teller activity.

As part of the design, integrated systems often employ data base management technology. Their processing structure may use combinations of batch, on-line, or memo posting methods. See Chapter 25 for additional information on FFIEC SP-4: Supervisory Policy on Large Scale Integrated Financial Software systems.

Integrated software systems are advantageous, because they:

- Increase efficiency and reduce unit processing costs through standardized operating techniques.
- Eliminate redundancy in data files.
- Provide tools to increase product lines and customer relationships.
- Enable financial institutions to meet competition generated from forces outside the banking industry.
- Improve the timely delivery of information throughout the institution.
- Allow more informed management decisions.

Managing the Project

A commitment to an LSIS sets the course of an institution's technology, management information systems (MIS), and delivery systems for several years. Although large scale integrated systems offer substantial advantages, their inherent complexity requires more formal development and maintenance procedures, specialized audit techniques, and senior management commitment. These are essential to the successful implementation and operation of large integrated systems.

As financial institutions convert to integrated software systems, many experience considerable difficulties. Some institutions spend millions of dollars and years of conversion and implementation time, only to abandon the project.

To avoid these difficulties, factors which should be considered by management, a full commitment to this type of project include:

- The financial condition and viability of the vendors when evaluating systems.
- The financial impact on the institution, in terms of not only the initial cost, but also the time and resources required for successful installation.
- If the system uses real-time data base technology, the cost of data backup and recovery measures, as the entire data base must be backed up simultaneously.
- The time and capability of a backup computer to test the disaster recovery plan of an LSIS.
- Whether SDLC methodologies need to be modified because of the increased complexity of the software and the difficulty of assuring system integrity (seemingly simple program changes can have unpredictable results in a multi-application system).
- Whether audit and control issues are adequate for real-time integrated systems.
- Whether system access is difficult to control and monitor, especially when using dial-up access.
- Whether audit trails address system-generated transactions sufficiently.

Management Responsibilities

The decision to acquire or develop in-house LSIS should be preceded by a strong and independent management planning process. This should include a thorough assessment of existing software performance. Also essential is a detailed analysis of additional capabilities necessary to accomplish the institution's strategic business plan.

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

The institution's board of directors should review the project often to maintain control over the complex process of implementation and to ensure completion within established parameters. Board reporting formats should be established at the beginning of the project. The board must continue its oversight responsibilities after implementation.

OPERATING SYSTEMS

Current generation computers differentiate between application programs and operating systems/supervisor programs. The operating system controls all input, output, and interrupts. It also controls program scheduling and hardware resource allocation.

The operating system:

- Increases system throughput by overlapping input and output operations with processing.
- Improves user turnaround by permitting simultaneous processing of applications.
- Simplifies implementation of new applications by providing general purpose utility programs, thereby reducing the number of programs that must be written.
- Assists programmers by relieving them of the burden of writing logical and physical input/output control instructions.
- Improves overall operational efficiency and control by providing:
  - Job scheduling.
  - Analyses for job accounting and computer system use.
  - Control over programs stored in the computer.
  - Control over access to and use of the data files.
  - Control over use of all hardware resources.

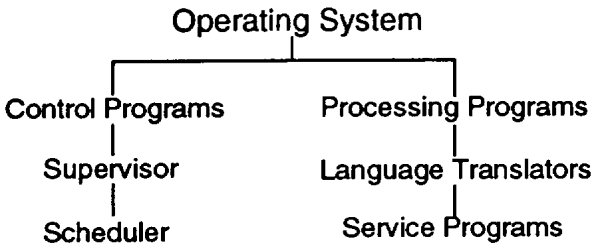
Most operating systems contain a significant variety of optional features. Specific features can be selected for implementation in individual installations. Since some features change the processing and can either add to or overcome controls, a record of them should be kept.

An operating system generally consists of the following programs (Figure 12-2):

-

Control programs. The control programs provide control over a continuous series of jobs, the workflow within the system, and the input/output operations. Control programs consist of two basic components:

Figure 12.2
Sample Basic Elements of an Operating System



- The supervisor program controls how computer system resources are used. It coordinates all processing to assure that each program receives the services requested. The supervisor program normally responds through an interrupt system and a specialized set of privileged instructions.

- The scheduler program accepts job instructions, allocates input/output devices, initiates the execution of processing programs, and maintains communications between the system and the operator.

For efficiency, only the control program and a few of the most commonly used service programs will reside in memory at all times. The resident memory portion of the operating system is sometimes referred to as the nucleus. All other service programs reside in a library, usually on magnetic disk.

Processing programs. Each operating system provides a comprehensive set of generalized programs designed to assist the user. Some of the current programs are:

- Language translators to assist programmers by translating application programs written in a high-level language into machine instructions. The majority of mainframe computer manufacturers provide the following language translators:

  - COBOL. This is an acronym for COmmon Business Oriented Language. This language is best suited for commercial or accounting functions.

  - FORTRAN. This is an acronym for FORmula TRANslator. FORTRAN is an algebraic language and is well-suited for scientific and engineering applications.

  - BASIC. This is a simplified language similar to FORTRAN. It is an acronym for Beginners All-purpose Symbolic Instruction Code. It differs from FORTRAN, since it can function in an interactive or conversational mode.

  - RPG. This is an acronym for Report Program Generator. RPG was originally indented to permit the user to write simple report programs with minimum effort. It is now used as a stand-alone programming code (RPG-II and RPG-III).

  - Assembler. This is a low-level language. Although difficult to code, it may result in more efficient programs. The use of Assembler language allows bit level data access and usually makes all machine instructions available to the programmer.

  - C. Although primarily a microcomputer or workstation language, it is gaining popularity in DEC/VAX systems because of its portability. An extension of C called C++, an object oriented program, is expected to gain popularity in the future.

- Service programs to provide routines for commonly performed functions. Examples include linkage editors, sort/merge, library maintenance, data management, and manipulation. These programs can be divided into two basic groups:

  - System service programs. These programs are called by the supervisor in response to interrupts. The user may, in some cases, change priorities or provide parameters, but does not execute the program or routine. Some examples of system service programs are:

    Open/close macro instructions for data files.

Program check and memory dumps.

Data file access routines.

Routines for loading and executing programs.

Job accounting routines.

System error checking routines.

Routines for allocating memory.

Spooling routines for input and output.

Queuing routines for entry of jobs and assignment of priorities.

Communication programs in on-line environments.

- Utility programs. The following general purpose programs are initiated directly by the user:

  · Sort/merge programs for sorting and merging data files together.

  · Linkage editor programs to link programs that have been compiled or assembled by a language translator. (When a program is too large for memory, the linkage editor can be used to divide the program into overlays.)

- Data file manipulation, copy, or print programs.
- Program library maintenance routines.

PROGRAMMING PERSONNEL

Application Programmers

Application programmer activities should be clearly defined. Access to programs outside the programmers' individual responsibility should be restricted. Maintenance expertise should exist for each major application, and responsibility assigned to specific programmers. Programmers not assigned to maintain or develop specific programs should have access restricted only to such programs.

If application programmers are allowed to write programs in low-level languages, such as Assembler, they should not be permitted to execute instructions generally restricted to the operating system.

Programmer use of storage dumps should be restricted, so that only those persons authorized to use specific dumps have access to them. Storage dump listings and program source listings used by programmers should be secured when not in use and destroyed when no longer needed.

Systems Programmers

In many organizations, a distinct group of highly skilled programmers must maintain operating systems, teleprocessing control systems, data base systems, and develop supportive applications. Such programmers are generally known as systems programmers.

Larger data centers may refer to their systems programmers as the technical support group. This group serves as liaison with manufacturer system software support personnel, application programmers, and the information systems operations staff. Group responsibilities for computer operations support include:

- Controlling program libraries and data sets.
- Maintaining operating system software and data base software.
- Identifying access methods.
- Installing other support software for use by operations, systems, and programming personnel.
- Allowing add-on systems, such as ATMs, to function.

The complexity of the technical support activities hinders the effective monitoring systems programming efforts. Written standards should be developed and enforced to monitor and control all programming activities. A clear distinction between the application programming and systems programming duties should exist.

PROGRAM SECURITY

Strict security should be maintained over access to and use of computer programs with such security

being physical and/or logical. 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 main-tenance, inquiry, and new accounts. Reference SP-4. Procedures should restrict unauthorized access to:

- Application programs.
- Operating systems programs.
- Data files.
- Documentation.
- Computer equipment.

In addition, periodic supervisory review of activity logs, time records, and other reporting techniques can be used as a monitoring technique. Specially designed software programs may be used to flag exceptions or changes to libraries.

At least three proprietary program librarian systems offer additional techniques to monitor program security. These systems can protect source and object libraries, maintain program version numbers, produce system activity logs, retain a chronological record of actual program coding changes, and restrict operator access to unauthorized functions. Since program development or modifications also can be performed from microcomputers after downloading program files from the mainframe, at least one librarian system offers increased monitoring of accountability for this type of end user access.

Systems also can alter or delete programs or data. This capability is contained in utility programs that are usually supplied by the manufacturer. Systems utility programs are valuable tools when used during program debugging, file maintenance, cataloging, or even daily operations of the data center. However, certain programs can be used to alter core storage, data files, and object code; enter the supervisor state; and catalog, purge, and rename programs. Such action can be justified occasionally when data becomes garbled or can be unjustified when an improper action is contemplated. Most computer manufacturers supply these programs as part of the operating system. Programs, such as DITTO, IMASZAP (Superzap), IEBGENER, MSHP, IEBRENAM, IEBUPDAT and IMASZOT, should be controlled to prevent unauthorized use. Manufacturer utility program manuals can be consulted to determine programs to be controlled.

Unauthorized use of system utility programs can be controlled in several ways. These controls, however, will not be effective, if they unnecessarily impede operations. System utilities can be controlled by:

- Removing utility programs that have data or program altering capabilities from the system catalog. Place these specific utilities, which are on machine-readable media, under the physical control of the shift or operations supervisor.

- Installing a password system on all program libraries, including the system utility library. If password protection is used, measures must be taken to control access to passwords. Passwords should be changed periodically.

- Using automated librarian systems. Several automated librarian systems that provide program security are available from equipment manufacturers and software vendors. Such programs restrict access to the program library. They can produce daily reports identifying each program that was accessed and any program changes that were made.

Even the most sophisticated program security system will fail, if management does not establish, implement, and maintain adequate internal and operating controls. Standards and procedures for all aspects of program development, processing, and maintenance are necessary. These must identify control responsibilities and processes for documentation, review, and approval of various programming activities. Supervision of these functions is imperative for establishing and maintaining program integrity.

DOCUMENTATION STANDARDS

The value of documentation is derived from its accuracy, timeliness, and completeness. Well-documented systems are easier to maintain and

convert to new systems. Good documentation also facilitates the rotation of personnel/separation of duties, and supports the continuity of operations in the event of key personnel turnover. Program documentation is often time consuming and

regarded as non-creative. However, it is the most convenient method of determining program functions. Furthermore, inadequate documentation can often lead to a lack of administrative control.

There are no universal documentation standards. The American National Standards Institute (ANSI) has approved standard number 1063 developed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) which applies to software user documentation; however, this standard does not apply to design, development, or changes which involve modification of source code. Effective documentation procedures require the involvement of financial institution and information systems management.

As a starting point, common practices in the financial institution information systems industry should be reviewed. The development of documentation standards could be a process of adaptation rather than origination.

The development of documentation standards will require analysis of the financial institution's current information systems environment and projections of future requirements. After the general scope of the documentation is defined, the format must be organized in a logical manner. Various methods and procedures creating documentation should be investigated. Each step of the process should be reviewed and evaluated. When documentation is complete, plans should be implemented to update and revise it as the financial institution's needs become more sophisticated and diverse. The standards and procedures manual should contain standards for documentation. If the institution allows end user modifications of programs from microcomputer or LAN systems, the institution also should specify the level of user documentation which is required.

Regardless of the method used by the installation to organize its operating standards, procedures and requirements for developing and retaining program documentation must be included. The essential elements of program documentation follow.

APPLICATION SOFTWARE DOCUMENTATION

Each application in production should be supported by a complete set of program documentation. For each application, documentation should contain a problem definition, application system and program descriptions, operator and user instructions, and records of acceptance of the system. Access to the documentation should be restricted. Personnel should have access to only those sections of the documentation directly related to their job functions.

The following further describes documentation sections:

- Problem definition – Provides a clear, logical and formal record of the problem to be solved. The contents of the problem definition may include many of the concepts in the below example. (Figure 12.3)
  - Project background and project request (usually by the potential user).
  - Minutes of steering committee meetings or copies of policy decisions relating to the proposed job.
  - A problem statement defining the purpose of the proposed program.
  - Estimated and incurred costs.
  - Programmer-hours forecast and incurred.
  - Basis for decisions.
- Application system description – Provides an overview of the total application and ties together the individual computer programs within the application system. The application system description may be subdivided as follows:
  - System flowchart. Indicates the source and nature of the input, appropriate automated and manual operations, and the nature and disposition of output. The system flowchart illustrates the flow of the work through the application system (Figures 12.4 and 12.5).
  - System narrative. Describes the general outline of the application system, the related environment or computer system in which the program will operate, the operations it affects, its users and the interrelationship of its uses.

  Record layout schematics. Reflect the format of data items on cards, magnetic tapes, paper tapes,

or disk tracks. Disk and tape layouts contain additional information on record size, blocking factors and the layout and contents of internal labels (Figures 12.6).

- Print layouts. Reflect data items output to print, showing columns, column headings, number of lines, spacing, and report titles.

- File description. Reflects the collection of related records that form a file for the information system processing application. A file description might logically describe an interim file, such as the sorted demand deposit transaction file, in order to further define requirements for processing. It also may logically describe the demand deposit master file for the same reason.

- Special code. Identify various types of transactions, activity accounts or other special indicators.

- Control function. Describe the accounting and operating controls. On-line systems should include a complete security narrative and a list of users having authority to inquire and update. Methods needed to maintain security also should be described. Restart and recovery procedures should be detailed if applicable.

Figure 12.3
Sample Problem Definition Statement

DATE_____ PAGE_____
REFERENCE #_____
PREPARED BY _____
REVIEWED BY _____

Problem Statement

Payroll Systems Flow

Problem

The daily time sheets are added each day. At the end of the week all time sheets are checked for completeness. Each time sheet must be filled out completely with all hours charged to specific jobs. At the same time the time sheets are checked, they are sorted by employee number.

Hours are added for each employee and posted to the payroll register. The total of all hours posted is checked against the add tapes to insure accuracy of the posting. Each employee's gross pay is determined with the aid of the payroll master file and is posted to the payroll register.

All deductions are calculated for each employee and posted to the payroll register. Net pay is determined for each employee and posted to the payroll register. The payroll master file is updated to include the current period's payroll.

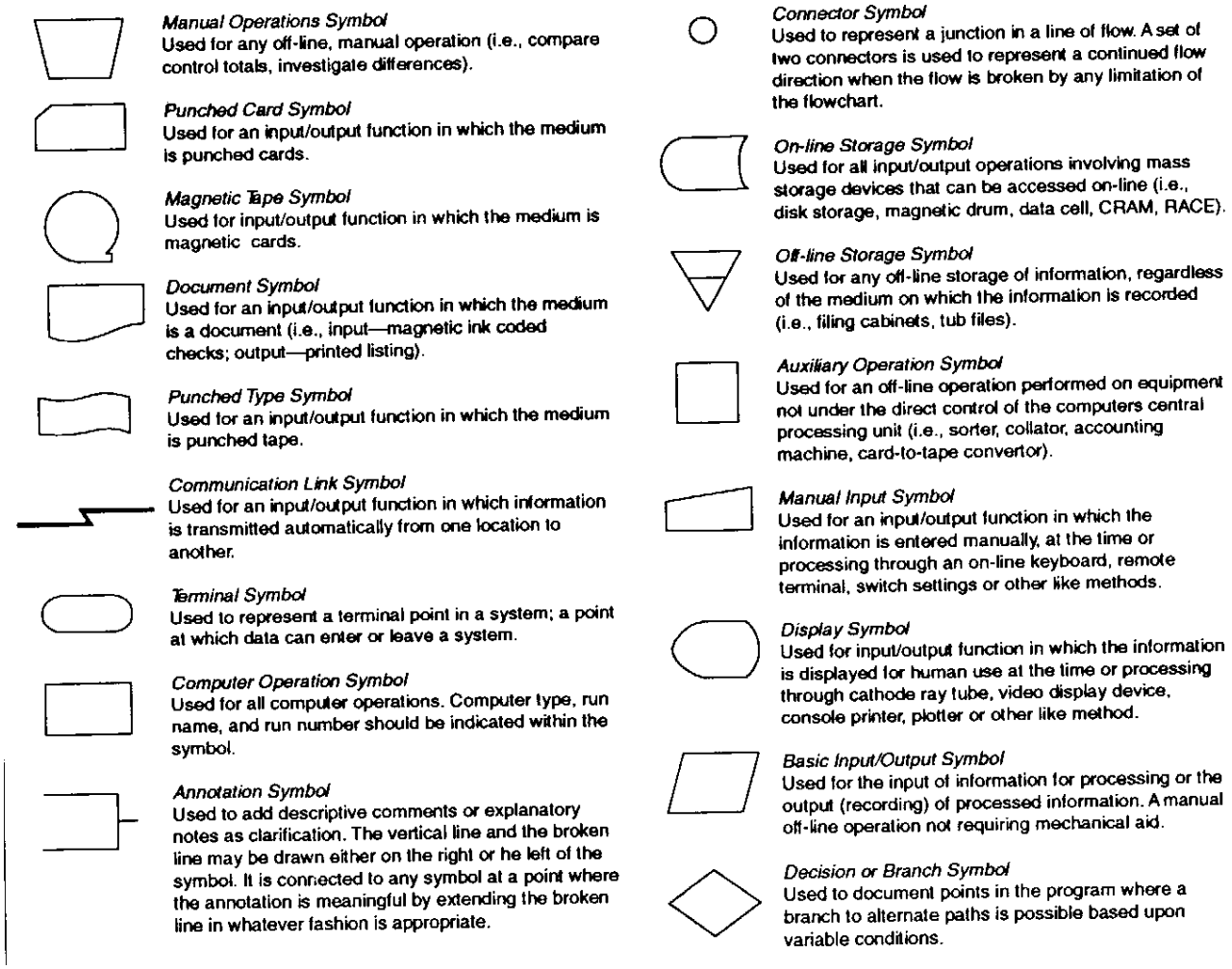
Description of Input

The principal input documents to the payroll are the daily time sheets and the updated payroll forms showing new employees, pay changes, etc. The updated payroll forms are used to updated (correct) the master payroll file prior to starting the payroll.

Description of Output

Payroll checks are typed from the information contained in the register. Net pay totals of the typed checks and the register are compared to be sure the typing is accurate. The payroll register and daily time sheets are filed by payroll date.

Figure 12.4
Sample Flowchart Symbols



- Program description – Describes the details of the individual programs and should include:
  - Program flowcharts (if applicable). Present the logic and flow of the program, subroutine or module within a major program. This documentation also may be termed a block, a logic diagram or logic chart. Flowcharts may be necessary for complex sections of programs and for programs written in low-level languages. Automated flow chart packages are available which will either automatically flow chart a program based on source code or will enable the programmer to flow chart a program without the need for drawing the chart manually.
  - Decision tables (if applicable). Supplement or replace flowcharts for description and documentation of more complex programs. The decision table is a tabular representation of the program logic that specifies all conditions and action relationships according to a set of user defined rules (Figure 12.7).
  - Table description. Present sets of data items

stored in tables for reference at various points in a program. Description of such tables and their value are a necessary part of documentation.

- Flags and switches. Describe program tests for specified conditions which are either present or changed, depending on the flow of instructions dictated by the logic of the program.

- Program change and system modification forms. Describes a change to an application program, application system or the operating system showing the result, benefits to the user and proper authorization. A detailed explanation should be maintained (Figures 12.8 and 12.9).

- Program listing. Should contain nontechnical comments and meaningful data names. Program listings and narratives are the most basic items in program documentation. Many of the other elements of program documentation can be derived from the program listing. The listing should be updated when programs are changed. With paper reduction generally mandated, institutions are either using microfiche for listings or retaining source listings on-line with appropriate access controls in effect.

- Programmed controls. Describes all editing performed by the program.

• Operator instructions – Explain how a particular job is performed and how operators should respond to certain system requests or when halt conditions

Figure 12.5
Sample System Flowchart

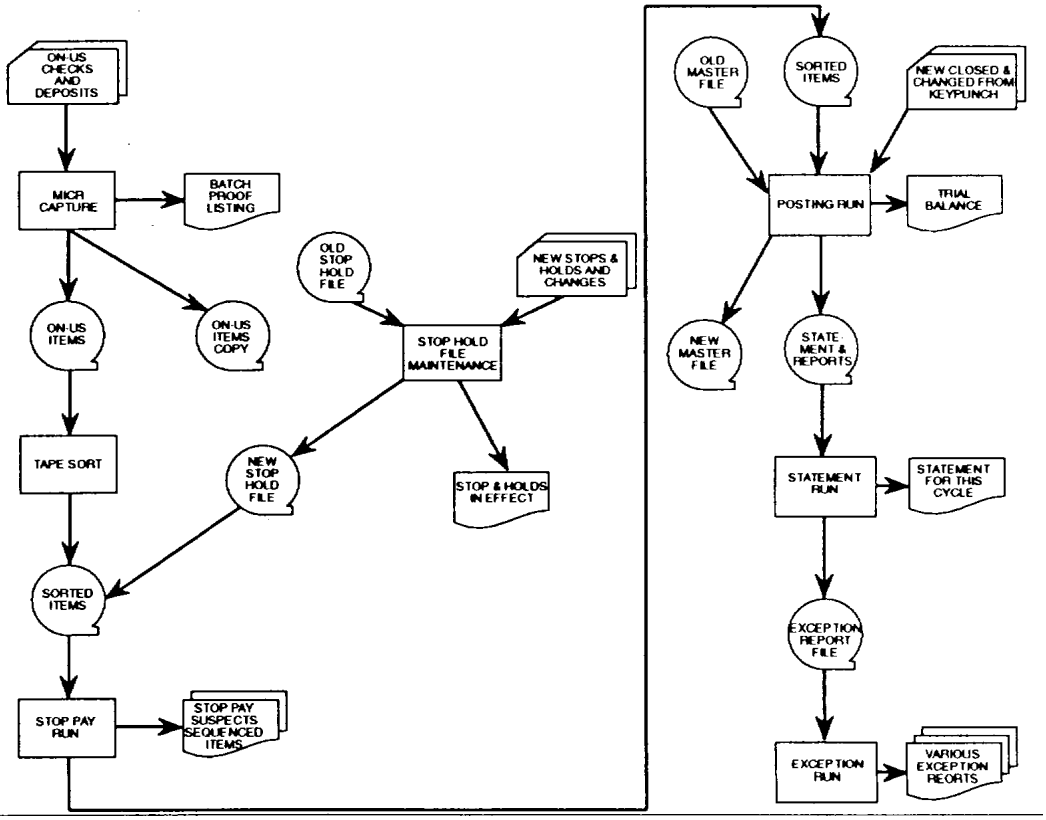
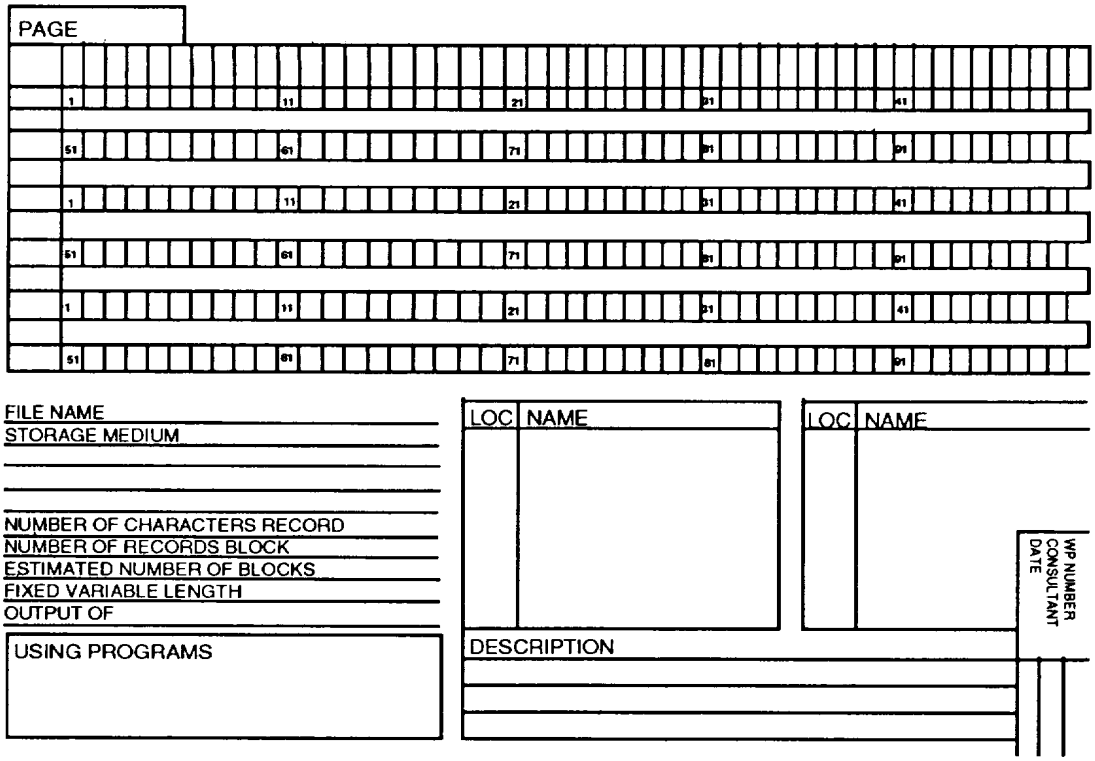


Figure 12.6
Sample Record Layout



occur. This documentation should include only information pertinent to the computer operator's function; program documentation such as source listings, record layouts, and program flowcharts should not be accessible to the operator. Operator instructions should be thorough enough to permit an experienced operator who is unfamiliar with the application to run the program successfully without assistance.

- User manuals (see the section on user manual documentation).

- Record of acceptance – Documents the formal acceptance of the completed application program modification. At a minimum, formal acceptance should be obtained from:

  - User department. Should indicate that test results have been reviewed and that the system meets specifications.

  - Information systems department management. Should indicate review of test results and control functions.

  - Audit department. Also should indicate review of test results and audit/control functions.

  - Information systems operation. Should indicate review of run instructions and acceptance of any additional hardware demands and run time.

  - Documentation librarian function. Should indicate review of documentation for completeness and compliance with standards.

When developed or modified in-house, operating system software must be supported by comprehensive programmer and user documentation. Regardless of the source of operating system and other support software, standards and procedures for maintaining such documentation must be developed by the financial institution.

MAINTENANCE OF DOCUMENTATION

The documentation librarian function is responsible for the control, retention, storage, and distribution of master documentation files. The exact procedures

Figure 12.7
Sample Decision Table

DATE _____ PAGE _____
REFERENCE NO. _____
PREPARED BY _____
RECEIVED BY _____

DECISION TABLE _____

_____

STUB	ENTRY																			
CONDITION	RULE NUMBER																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ACTION	RULE NUMBER																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

PAGE ____ OF ____

Figure 12.8
Sample Program Change Request

DATA PROCESSING PROGRAM CHANGE RECORD	
Program Name or Description	Change Number
Program No.	Date Change Effective
Change Initiated By	Date
Change Request Approved By	Date
Description of Purpose or Reason for Change	
Description of Changes Made (and Effect on this and Other Programs)	
Change Made By	Date
Change Tested By	Date
Change Posted to Run Manual By	Date
Change Posted to Operator Instructions By	Date
Review of Changes By	Date

Figure 12.9
Sample Change Request Form

PROGRAM CHANGE REQUEST

REQUEST NO.	DATE COMPLETED
PROJECT NO.	DATE IMPLEMENTED
DATE RECEIVED	DATE CANCELLED
APPROVED BY	ASSIGNED TO
DATE APPROVED	DATE ASSIGNED

REQUESTOR — COMPLETE ITEMS 1-5; SEND TO SYSTEMS LIBRARY, 2-95.

1. REQUESTOR'S NAMES | REQUESTOR'S DEPARTMENT | MAIL CODE

2. NAME OF APPLICATION TO BE MODIFIED | DATE

3. STATE REQUEST AND REASONS (INCLUDE COST SAVINGS OR OTHER BENEFITS)

4. DESCRIBE THE MODIFICATION IN DETAIL (IF NECESSARY, CONTINUE ON BLANK PAGES)

5. OBTAIN THE SIGNATURE OF YOUR SYSTEMS DEVELOPMENT PRIORITIES COMMITTEE REPRESENTATIVE TO AUTHORIZE THE SYSTEMS DEVELOPMENT DIVISION TO STUDY AND ESTIMATE THE COST OF IMPLEMENTING THIS REQUEST.

PRIORITY REPRESENTATIVE'S SIGNATURE

SYSTEMS DEVELOPMENT DIVISION

PROJECT LEADER	MANPOWER COST	MACHINE COST	TOTAL COST	DATE	UNIT	DIV.

APPROVED BY: PLEASE INITIAL, DATE AND FORWARD WHEN ALL APPROVALS ARE OBTAINED. RETURN TO SYSTEMS LIBRARY 2-95. IF YOU DO NOT GET APPROVAL FOR THIS REQUEST, RETURN IT TO PROJECT LEADER NAMED ABOVE WITH A MEMO STATING THE REASONS FOR DISAPPROVAL.

REQUEST	MAIL CODE	INITIAL	DATE	ADDITIONAL APPROVALS NAME	MAIL CODE	INITIAL	DATE
PRIORITY REPRESENTATIVE							
REPORT COORDINATION							
CENTRAL DATA PROCESSING							
AUDIT DEPARTMENT							

performed depend on the size and complexity of the data center and if the documentation is maintained on paper, on-line, or a combination.

The extent of the librarian function depends on the scope of information systems activities, the frequency of reference to library materials, whether processing functions are centralized or decentralized, the internal structure of the information systems department, and the medium on which the documentation is maintained. Specific librarian functions may include:

- Review of documentation at system development time to ensure adherence to standards and appropriate authorization of exceptions.
- Control and storage of acceptable documentation.
- Handling of documentation revisions.
- Notification and distribution of documentation to interested or authorized parties.
- Current maintenance of all documentation.

In small installations, the documentation library area may consist of a few filing cabinets in the programming area, maintained by a clerical person or the programming supervisor. In larger installations, it may be a separate area staffed by a full-time librarian particularly if paper documents are required for all forms of documentation. Such libraries may employ control and access procedures

similar to those exercised over data file libraries. Now that many institutions are using on-line facilities for the bulk of documentation, filing cabinets may be appropriate to maintain documentation. However, in all instances, the documentation library or storage areas should be secured to prevent unauthorized access.

Documentation must be kept current. Standards for documentation must specify the authority and techniques for maintenance and control; responsibility for maintaining program documentation must be assigned.

Actual techniques for revising the documentation will depend on its structure and changes to it. Documentation can be revised either by programmers or by technical writers. Explicit rules for amendments must be established to prevent needless paper accumulation. Accordingly, provisions must be made for:

- Changes which can be made directly on existing paper documentation (if applicable) without making the end result illegible or unintelligible.
- Additions which amplify, clarify, or augment existing documentation without making the present content obsolete.
- Changes which are a complete or a partial replacement of existing documents.
- Changes which can be made to on-line documentation.

Documentation plays such a vital role that procedures to duplicate essential portions should be established. The duplicates should be retained in an off-premises storage facility and must be periodically updated. If documentation is on-line, the back-up of this information on magnetic media can be accomplished easily.

USER MANUAL DOCUMENTATION

User manuals enable the user to understand, approve and operate the system. Lack of user involvement may result in the user:

- Instituting inadequate remedies to problems, thus negating certain controls within the system.
- Contending that the whole system is defective.
- Placing complete reliance on the information systems department for controlling the operation of the application.

Continuing user involvement is of primary importance; therefore, user aids or manuals are essential aspects of program documentation. The responsibility for writing user manuals and user manual standards should be established formally.

A user manual could be divided into two main areas: input and output. The manual should be written in simple, nontechnical language, and not directed to a particular audience. When necessary, illustrations should show proper completion of forms, workflow, and descriptions and explanations of reports generated. When forms are illustrated, they should contain representative sample entries and instructions keyed to those entries. Every transaction code should be described in sufficient detail to allow the user to fully understand how to use the application system. Output reports should include detailed explanations of special codes, flags and reconcilement procedures necessary to balance the report user controls. The output reports need to be reviewed periodically to determine if they are being used as intended, or if they should be modified or discontinued.

PURCHASED SOFTWARE DOCUMENTATION

A prime consideration in any purchased package is documentation. If a package is not well documented, the user will not understand the techniques and methods used. The package may be less effective and efficient as well as difficult to maintain if program changes are to be performed by the purchasing institution. The format and content of this documentation, however, probably will not be written according to the financial institution's information systems standards. The documentation of program packages under consideration must be reviewed prior to purchase to determine if the product generally meets the financial institution's minimum documentation standards. Such precautionary measures also should be applied to the purchase of standard utility programs, such as sort or merge programs.

Purchased software will be subject to subsequent modification by the user or vendor. All changes made to application programs and operating systems must be documented according to

prescribed standards. When contracts are written to include continuing maintenance of the software by the vendor, the vendor must have the technical and financial ability to perform this task. This is especially important for installations that do not have an adequate programming staff. Some vendors provide documentation on magnetic media and this information may be loaded into the on-line documentation system for reference purposes. A potential problem in documentation can arise if the purchased package requires modification before it is installed. It must be determined up front who will modify the documentation with the vendor and/or the purchasing institution involved in the process.

DATA BASE MANAGEMENT SYSTEMS

Data base management systems are playing an increasing role in modern information processing. A data base is a collection of nonredundant, interrelated data elements that are acted upon by one or more application programs. Data elements are organized to form distinct data files that are either relational, hierarchial, or network interconnected in nature. Data files are identified by a unique key, such as an account or employee number, and may contain pointers or indices to all of a customer's accounts. Data is accessed through a common software controller, commonly referred to as a data base management system (DBMS). Generally, the DBMS is provided by the manufacturer or an independent software vendor. Through the controller, an application program can access any relevant record regardless of its location or format. The data manipulation language (DML) interfaces between the application program and the DBMS to perform various functions such as opening a file, inserting a record, or changing data. An example of DML is IBM's Structured Query Language (SQL) which is used with IBM's DB2 relational database.

The sophisticated features of a data base, if properly designed, can greatly benefit a financial institution. However, a data base also can contain some disadvantages management should be aware of. Advantages and drawbacks include:

Advantages

- Reduction of data redundancy. In a multiple file system, the same data items are often stored in separate files. Such storage creates an updating problem since each file must be separately updated whenever a change to the data occurs. To the extent possible, a data base system only will store each item once, thus eliminating multiple updates and saving storage space.

- Program and data independence. Previously, it was necessary to define format and storage characteristics of data within each program. A data base system separates the physical storage and accessing functions. Therefore, the data base can change and grow without necessitating an update to each application program. In addition, the programs deal with data content rather than location. This independence can facilitate moving the applications from one computer to another.

- Standardized data definition and documentation. These functions are standardized by using a data dictionary and controlled by the data base administrator.

- Unlimited number of data relationships. Since pointers may be used to associate one file with another, the number of data relationships possible is unlimited. More data is therefore available to individual programs.

- Program development costs. A data base reduces the need for separate storage and retrieval procedures. Inconsistencies between individual files with redundant contents are reduced and program maintenance costs should decline with the elimination of some maintenance procedures.

Disadvantages

- Data integrity and data relationships. Since data items are normally stored only once within the data base, all users of a data item will access the same item. An incorrect data item will create an error for, and have a major impact on, all users. As the data base is enlarged, relationships each item has with the other items also increases. Therefore, those relationships must be defined accurately and each item in the relationship must always conform to its defined role.

- Problems for the auditors. Auditing a data base management system requires more sophisticated audit techniques. Traditional sequential file audit retrieval packages will not access data base management systems directly. Audit software

for data base systems now is available but a learning curve will be in effect.

- Cost offsets with data bases. Increased costs in some areas may offset any cost reductions in program development. Increased costs may result from:
  - DBMS development.
  - Additional equipment.
  - Increased planning.
  - New and elaborate controls, requiring a more sophisticated programming staff.
  - Changes and adjustments to meet technological advances.
- Data security or privacy considerations. Files for all applications are generally mounted and available to application programs at all times. This differs from batch environment files which are dismounted and secured in a library when not in use. Risk exposure is often heightened by diffusion of file security responsibility. In batch systems, the files are the property of the various user departments. In a DBMS, data belongs to everyone so that no one user is solely responsible for its safety. Thus, control over these files rests with a central authority – such as the data base administrator – who determines who has access and the level of access capability, e.g., addition, deletion, modification, or read only. Because the data is available to many users from numerous terminals, it should be determined if levels of access to key fields are adequately controlled to maintain certain security and privacy of data.
- Destruction of files. Since massive volumes of data are difficult and costly to copy, data base systems when updated often destroy old files. This makes it more difficult to backup such files and requires periodically dumping files and saving transactions. Because of the expense and difficulty of such backup techniques, only critical data may be backed up; other less critical data is subject to destruction and loss.
- Software failure/slow responses. Because a data base system is so complex, there is a high probability of breakdowns. Precautions to avoid breakdowns can add another layer of overhead to the software which can slow response time.

Types of DBMS

The main types of data base structures are:

•Hierarchical – represented as a tree with the root at the top and data located where a tree would branch.

Figure 12.10
Sample Hierarchical Data Base

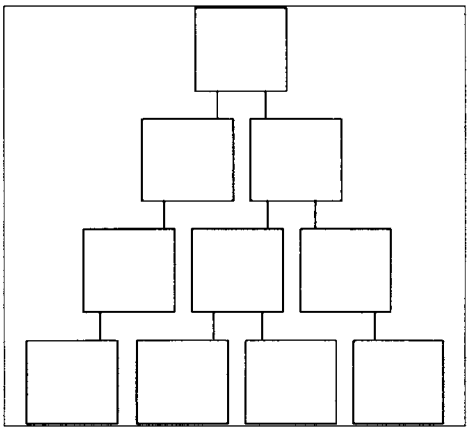
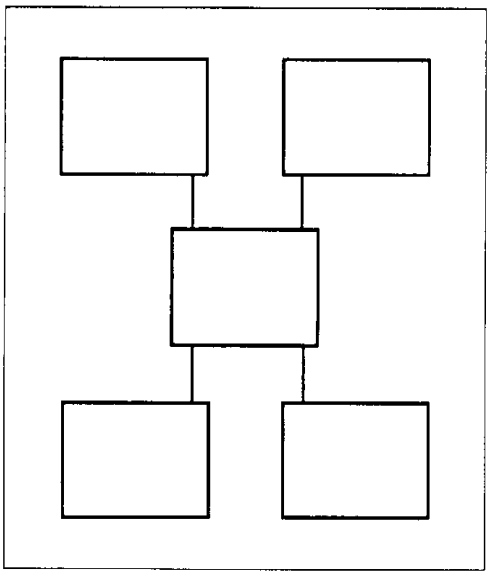


Figure 12.11
Sample Network Data Base



Similar to an organization chart, the lower data element is dependent on the one above it and a parent-child relationship can be envisioned as the data path. Each parent can have more than one child, but a child can have only one parent (Figure 12.10).

- Network – represented as links of parent/owner and child/member record types. Pointers can go in a forward or reverse direction and a child/member record can have more than one parent/owner. Within a network any data element can be connected to another one (Figure 12.11).

- Relational – represented as a table of columns and rows with columns corresponding to records and rows to fields. Paths or links are not pre-defined and no pointers are needed since relationships are defined at the data value level (Figure 12.12).

Refer to Figure 12.13 for examples of software for each data base structure. It is evident that relational data bases are becoming more prominent.

Data base systems traditionally have been centralized on one computer with data, programs and directories residing on a central processor. In a Distributed Data Base system, the data, program and directories can be spread among different processors and can be useful for organizations geographically dispersed or functionally diverse.

The essentials of data base security are:

- Data should be protected from fire, theft and other physical hazards.

Figure 12.12
Sample Relational Data Base

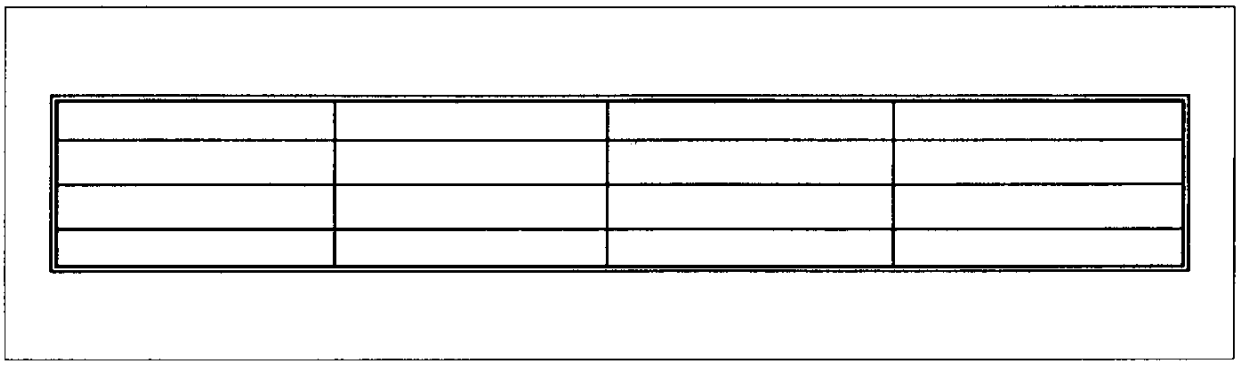


Figure 12.13
Example of DBMS Software

Hierarchical	Network	Relational
IMS (IBM)	CA-IDMS/DB	DB2 (IBM) (Computer Associates)
SYSTEM 2000 (INTEL)	TOTAL (Cincom)	SQL/DS (IBM)
	DMS 1100 (Unisys)	ORACLE (Oracle Corporation)
		RDB (Digital Equipment Corporation)
		CA-DATACOM/DB (Computer Associates)
		ADABAS (Software AG)
		MODEL 204 (CCA)
		INGRES (Ingres Corporation)
		INQUIRE (Infodata Systems)

- Data should be reconstructible to recover from destruction or loss (intentional or accidental).
- Data should be auditable for prompt detection of loss.
- The system should be tamper proof to prohibit programmers from bypassing controls.
- Users must be identified before being granted access.
- The system must be able to check that user actions are authorized.
- User actions should be monitored so that suspicious or unauthorized behavior can be investigated.

Threats present in all processing environments may be heightened by certain features of data base systems. These threats include:

- Deliberate internal threats.
- A trapdoor or window built into the system by a programmer. Provisions must be made for flexibility in the operating software, particularly in a system as complex as data base management. Since this software must be programmed for change, it is vulnerable to unauthorized attempts to penetrate the system.
- Dumping portions of core storage to obtain sensitive information, codes, passwords, etc. (This could be a profitable mode of attack because of the exposure of all files, and the heavy reliance on access codes to control input to the system.) A countermeasure is to encrypt sensitive information so that it is meaningless if dumped directly from storage.
- Misuse of another person's authorized access code, password, etc.
- Deliberate external threats.
- Obtaining access codes or other restricted data by obtaining copies of hard-copy output from trash cans, dumpsters, etc.
- Obtaining access codes or other restricted data by wiretapping.
- Accidental threats.
- Faults in the data communication system leading to erroneous data in the data base.
- Hardware or software failures leading to a breakdown of a built-in security feature. For example, secret data – such as passwords – may be printed as part of a core dump during an abnormal termination or a recovery.

Program Control

Data base management systems must rely heavily on software controls (as well as terminal hardware and physical controls) to compensate for loss of library controls present in the normal file-based systems. Software controls are divided into:

- Authorization controls – Specify whether access will be granted to the system in general, and to individual programs, files, or records. Also specify the functions that can be performed, e.g., read, write, modify.

- Processing controls – Include edit checks, such as validity tests, reasonableness tests, range and limit tests, and produce a full audit trail.

Control Differences Between Data Base and File Systems

File systems may use many physical controls that are not as readily available in data base systems. Therefore, data base systems rely more heavily on control over access to the input devices and on internal software controls. These controls include:

- Controls over input:
  - Physical terminal locks.
  - Locks on communications link with computer.
  - Terminal identification code/procedure.
  - User identification code/procedure.
  - User security code or password.
- Internal software controls:
  - Program locks (specific users may be prohibited from accessing specific programs).
  - File locks (specific users may be prohibited from accessing specific files).
  - Record or field locks (specific records or files may be restricted from access by specific user).
  - Tests of result (the processing result may prohibit both further action and the transmission of the result back to the user).

Files that require a high degree of security can be maintained on disk packs separate from other data base files. They can be mounted at only certain times of the day when high-security jobs are scheduled to run. When dismounted, they can be protected by rigorous security measures.

If it is not practical to copy large volumes of data for backup, or if multiple generations of files are not produced by the system, it is still possible to provide backup. Destructively updated files should be dumped periodically with the related transactions for the period between dumps. The files may be recreated from the last dump. However, a large data base usually will not be copied in its entirety. Therefore, it should be divided into vital and nonvital records and files, with emphasis placed on copying the vital information.

Certain data may change so infrequently that it is rarely copied and can be easily updated from transaction records. Some systems keep duplicate copies of critical file data and update both copies. If one file becomes unavailable or damaged, the second copy is immediately available. This may be important for certain critical files in a real-time system. However, the technique provides no protection against program errors since both copies can be damaged by the faulty program. In this case, it will be necessary to reconstruct from earlier file copies.

Data Base Administrator – Duties

The data base administrator serves as arbitrator and mediator in the development, use, and maintenance of the data base. The administrator coordinates the activities of the organization as they impact on the data base.

Specific functions of the data base administrator include:

- Data definition:
  - Naming data item types.
  - Detailing data items in the data dictionary.
  - Combining data items into groups.
  - Establishing the logical relationships between groups.
  - Establishing retention periods.
  - Establishing standards for data records and

files used by programmers.

- Data base design:
  - Physical structuring of data on media.
  - Developing access methods.
  - Designing restart and recovery procedures.
  - Developing security measures and techniques for maintaining privacy.
- Data operations:
  - Investigating all data errors.
  - Supervising restart and recovery operations.
  - Supervising reorganizations of the data base.
  - Controlling and documenting changes to the data base and educating users.
- Security:
  - Investigating all known security violations;
  - Investigating suspicious activity noted on exception reports.
  - Establishing an authorization hierarchy, i.e., who is entitled to access what data.
  - Modifying security codes, passwords, etc., as required.
  - Monitoring compliance with security procedures.
  - Conducting periodic security audits to test compliance.

The data base administrator may have one or more assistants to handle detail work, or the overall function may be divided among several people of relatively equal authority. The latter concept is particularly sound since different talents and temperaments are needed for designing operations and overseeing their day-to-day performance.

An effective separation of the data base administrator's duties must exist. Although this person is the guardian of the installation's information, access to application-related data should not be allowed. Access to source listings and other application program documentation also should be controlled.

Data Dictionary/Director System (DD/DS)

A data dictionary is a central catalog containing source data definitions for an organization. It also includes:

- Information confirming the existence and availability of data.
- Precise data item formats, segments, and other data base design mechanisms.
- Computerized and non-computerized data, conventional files, and data bases (the current state of data dictionary development normally includes only data base information).
- Object data definitions plus physical storage locations and data access methods.

Although most DBMS have built-in directories that function separately from the DD/DS, a DBMS generally does not store source definitions and usually maintains object definitions that relate to the data base only. A DD/DS may contain the source location for both conventional files and the data base and maintain some object definitions that are not always found in a DBMS, i.e., security access control methods at the data item level. Therefore, it tends to supplement rather than duplicate the library features of a DBMS. Data dictionaries can be either active/-integrated or passive/non-integrated. Active DDs are updated automatically whenever a change is made in the DBMS whereas passive DDs are non-integrated and must be maintained separately.

Standards and procedures must ensure that changes to the DD/DS will be monitored, documented and communicated to the proper personnel. Changes must be:

- Authorized through the data base administrator.
- Approved by users.
- Amended in user documentation.
- Adequately tested for impact on usage and linkages.
- Reviewed to ensure that audit trails and controls are maintained.

Data Base Monitoring

An essential feature of a data base system should be adequate transaction logs or journals. Some of the items that may be recorded and possible uses of such entries appear in the Sample System Protection and Auditing Logs as seen in Figure 12.14. These logs should be detailed enough to facilitate recovery from minor hardware failures, software failures and incidents where data base files have been damaged or destroyed. They should include the application transactions and the administrative and operator messages accompanying the transmission during processing.

In addition, a log or journal provides an audit trail to trace the history of a transaction and investigate the

Figure 12.14
Sample System Protection and Auditing Logs

Key
✓ = Yes
P = Possibly
I = At specified intervals

Functions:	To provide an audit trail for an auditor to follow the history of a transaction	To permit recovery when it is found that a user has incorrectly updated or deleted a record	To investigate the causes when a record is found to be faulty	To assist recovery from massive file destruction	To assist in correcting the file when a program has been damaging data	To correct false information which has been sent to system users	To monitor procedural violations to highlight possible breaches of security	To assist in correct recovery from a system failure	To monitor the way the system is being used (as an aid to design)	To recover from the loss of a file-action journal
Transaction journal										
Incoming inquiry transaction						✓			✓	
Incoming update transaction	✓	✓	✓			✓		✓	✓	✓
Transaction type		P	P			✓	✓		P	
Transaction number	✓	✓	✓			✓		✓		✓
Originating terminal	✓	✓	✓			✓	✓	✓	✓	✓
Originating operator	✓	✓	✓			✓	✓		✓	✓
Time and date	I	I	I			I	✓	I	I	I
Response to inquiry transaction						✓			✓	
Response to update transaction	✓	✓	✓			✓			✓	
Indication that response was received correctly	✓	✓	✓			✓		✓		✓
Procedural violations on input							✓			
Record of start and end of file reconstruction									✓	
Note of completion of update									✓	
File-action journal										
Transaction number	✓	✓	✓		✓					
Time and date		I	I	✓	I					
Addresses of items updated	✓	✓	✓	✓	✓					
Contents of items before they are updated			✓	✓	✓					
Contents of items after they are updated	✓	✓	✓	✓	✓			✓		
Note of completion of update	✓	✓	✓	✓	✓			✓		
List of programs used for update			✓		✓					
Full contents of any records created			✓		✓					
Full contents of any records deleted			✓		✓			✓		
Details of any indices opened or closed			✓	✓	✓			✓		
Procedural violations deleted during update or processing							✓			
Contents of times corrected before correction	✓		✓	✓				✓		
Contents of times corrected after correction	✓		✓	✓				✓		
Indication of start and end of correction run	✓		✓	✓				✓		

The above information may all appear on the same journal.

cause of an error. The log also can highlight system utilization data and procedural violations that may indicate security breaches.

Some of the more advanced DBMS provide such logging features automatically; in others they are optional or must be developed by the user. More sophisticated control features provide automatic shutdown of disabled components and automatic transfer of functions to properly operating components.

COMPUTER–AIDED SOFTWARE ENGINEERING (CASE)

A software development technology known as Computer-Aided Software Engineering (CASE) may be used in financial institutions with large systems and programming staffs. CASE is used to automate software development process and maintain software systems in order to reduce programming costs, increase productivity, and produce reliable systems that satisfy users' needs. CASE technology provides a structured approach to designing information systems that meet business needs, manage information and share programming resources.

CASE uses a variety of process-modeling tools to automate systems design in all phases of the systems development life cycle (SDLC), e.g., data flow diagrams, structure charts, structure diagrams, data model diagrams, work breakdown structures, etc. Other products or tools provide the capability to create working models of a system's data entry screens, as well as layout of reports, for prototype testing by user departments. Structured system documentation can be automatically created in both hard copy and electronic form throughout the design and testing process.

CASE tools may be used separately or in an integrated fashion to reduce redundancy and increase coordination between programming tasks. The use of CASE tools in the early or late stages of the SDLC process are frequently referred to as UPPER CASE tools or LOWER CASE tools as described below.

- UPPER CASE refers to tools used in the early phases of systems design that relate to the requirements, analysis and design portions of SDLC.

- LOWER CASE refers to tools used in the later phases of the SDLC cycle that relate to natural language programming, documentation, code generators and testing.

CASE technology is often viewed as a solution to reduce software development problems. However, if not used with care, CASE tools can increase rather than reduce the risks associated with software development. Senior management and MIS directors need to be aware of these risk areas and controls.

Some common risk areas associated with the use of CASE technology are:

- Highly structured systems development – Institutions may move too quickly from an unstructured development approach to a highly structured CASE environment. CASE technology can be a radical change in the way systems are developed and tested. Systems and programming staffs may not adopt the processes necessary to implement CASE technology. Replacement of the old methods or simply implementing a methodology where none existed before cannot be accomplished quickly. Full CASE technology is generally implemented over a period of time to ensure staff and user departments are adequately trained in CASE.

- Change controls – An institution's use of CASE tools may affect the integrity of change controls in the institution's SDLC. The CASE products must be installed and administered properly. Generated code must be controlled by a sound change control process to assure it does not bypass control features that would allow a mismatch of source and object code.

- Unclear purpose – Management may fail to identify and quantify the purpose of acquiring and using CASE tools.

- Lack of standardization – CASE tools are not standard among vendors. CASE tools from one vendor may not be able to link to CASE tools from another vendor in the various stages of the SDLC. New tools on the market offer some integration, but only if the complete set is purchased. Typically, links between CASE tools and existing organization databases, dictionaries, and programming tools are inadequate, if they exist at all.

- Loss of CASE repository files – If critical files are destroyed, lost, or corrupted, the ability to regenerate any software may be lost.
- Project Selection – The project selected for

proving the value of CASE tools can be critical to the long term acceptance of CASE technology. The initial project should not be one that is critical to the organization, has high visibility, and short deadlines since there is a high learning curve during the transition to CASE tools. Likewise, attempting to use CASE tools to rescue a project that is over budget and late can be a mistake.

- Change in development process – Implementation of CASE programming tools will fundamentally alter the organization's software development culture and processes. Traditional SDLC concepts and procedures will have to be changed to take advantage of CASE. CASE methodology is highly structured and generally requires more discipline than developers and programmers may have been used to.

- High initial cost – CASE tools and associated staff training can be costly. Costs may appear to be initially high when weighed against early results before personnel have learned to use the tools efficiently and attained expected results.

- Management commitment – CASE cannot be implemented halfheartedly or part time. It requires a clear and strong management commitment and direction for success.

- Volume of output – A significant amount of documentation is generated when using CASE technology. The resources required to keep up with successive generations of documentation in order to know which change is in effect may require more staff time than expected.

- Training – Learning how to effectively use the new CASE tools requires a significant commitment of resources. This can lead to providing limited or no training in the hope that self-instruction will be sufficient; however, this is rarely the case.

In order to reduce the above risks and ensure maximum benefits, management should consider the following controls. These controls should not be regarded as all-inclusive nor should they be viewed as applicable in every situation.

- Clearly identify purpose and criteria for CASE Tools – Unless there is a clearly defined reason for acquiring CASE technology and specific requirements which must be met, there is reduced likelihood that it will be used efficiently or effectively. Often a cost/benefit analysis will help to clarify purpose and goals. Selection criteria should be determined prior to vendor discussions.

- Integrated CASE tools – Since CASE standards are incomplete today, the best way to ensure a smooth and automated interface between various tools is to consider purchase of CASE tools for the various stages of the SDLC from the same vendor and insist on demonstrable compatibility. If only selected CASE tools are going to be used, vendors should be selected that offer a full range of tools to reduce the likelihood that future CASE tools will be incompatible. If CASE tools are acquired from separate vendors, or one at a time, without regard to future interface, the likelihood that they will be incompatible is extremely high, with the result that a major benefit of CASE will have been lost.

- Protect the CASE repository – The CASE repository database should be backed up regularly, i.e., daily, secured from unauthorized access, and have controls over successive versions of data related to updated or revised development. The database usually contains all of the design and program data in order to generate and update software being developed. If this database is lost, the system progress to date and the ability to continue development also will be lost.

- Project selection – Until staff has experience with CASE tools, projects which have a low priority and are not time sensitive should be selected. If time pressures warrant, previous development methods can be reverted to. Likewise, projects which have high visibility run the same risk because of the pressure to meet deadlines. When CASE tools are not implemented successfully, benefits will not be realized, and acceptance will not be achieved.

- Determine systems development methodology changes – In addition to evaluating the changes in the development process required by the use of CASE tools, the flexibility of the existing policies and procedures to make necessary changes should be evaluated. Ample time should be allowed for changes to take place and expected benefits to be realized. It takes time for staff to learn to use the CASE tools effectively and efficiently.

- Quantify the increased productivity of CASE tools – The current productivity rate should be measured and compared with the productivity

rates of CASE tools under consideration. The return on investment should be calculated to indicate if CASE tools should be acquired.

- Promote involvement throughout the organization – Once management decides to implement CASE technology tools, this commitment must be communicated and shared throughout the organization.

  - Senior management commitment and support of CASE technology are essential for success. Management must clearly communicate their intent to implement CASE tools and be willing to accept a long-term payback rather than quick-fix results.

  - Programmers and systems designers using the CASE technology should understand what effect CASE tools will have on their work. They are directly affected and their level of acceptance (or lack of it) in learning new concepts can determine the success of CASE projects.

  - The internal audit department (IAD) should be involved throughout the CASE implementation project. In the early stages, IAD can evaluate the proposed changes to modify the SDLC processes. IAD also can evaluate how well CASE was implemented and suggest improvements. CASE tools often generate general documentation which can be used as part of any audit. Repository reports can give the auditor an understanding of the systems development process.

  - The users probably will see parts of the proposed system or an early prototype sooner than under the traditional SDLC development process. They should be prepared for that early involvement and be ready to actively participate in testing and refining early models.

- Volume of output – Output from CASE tools should be retained on electronic media rather than hardcopy wherever possible. Strict procedures should be developed to control versions of each generated system or subsystem. Only those documents that are essential for current development or historical purposes should be retained and the rest discarded. Documentation stored on electronic media should be backed up on a regular basis.

- Training – CASE tools cannot be learned effectively from manuals or do-it-yourself efforts. Professional training is essential for mastering the tools and moving quickly up the learning curve. The cost of trial-and-error development can be much higher with accompanying delays.

This section is intended to evaluate the quality of, and to determine the degree of compliance to, the standards and procedures applicable to the institution's systems development and programming (S&P) activities. The complexity of the S&P area could range from no in-house programming to complete systems development. The examiner should document any findings, especially those that do not satisfy the recommendations outlined in the 1996 *FFIEC IS Examination Handbook.*

Tier I

PROJECT MANAGEMENT AND CONTROL

1. Obtain applicable committee, management, and users' group minutes, and other written memoranda and instructions that govern the systems and programming function.

   Evaluate the supervision and project control procedures for management to maximize production and resource efficiency and identify and minimize risks in systems development and programming activities. Determine if the control mechanisms used by management are adequate by the review of :

   a. Automated project planning, monitoring, and production software aids used to help control and facilitate the systems and program development process.

   b. Project management reports that set forth the project goals and the current status of major projects, including the programming backlog.

   c. Cost/benefit analysis performed on all major systems development and maintenance projects.

   d. Information systems steering committee minutes or appropriate user committee involvement in setting project priorities and approval review of the development activities.

   e. Any other control mechanisms used by management.

STANDARDS

3. Obtain the "Systems and Programming Standards Manual", memorandum, and other written documentation that govern the activities of the systems and programming function, and:

   a. Determine whether the following written policies, procedures, and standards are adequate:

      (1) Application systems development.
      (2) Application program development.
      (3) Operating system maintenance.
      (4) Program change control.
      (5) Testing.
      (Program and system documentation.
      (7) Implementation.
      (8) Database management systems.
      (9) Backup and recovery.
      (10) Security controls.
      (11) Vendor software support.
      (12) Updating standards and procedures.

APPLICATION SYSTEMS DEVELOPMENT

4. Obtain or prepare a list of all automated applications currently in use or under development. Indicate if the applications were purchased or developed in-house. Also, indicate the person responsible for providing the maintenance support, and determine whether: (For IN-HOUSE developed systems, obtain and review documents generated from the system development process for a selected application system. Trace the documentation from the initial request through the post implementation review.

   a. All required documentation is present and sufficiently detailed to evidence complete compliance with established standards.

   b. The structure of the SDLC planning includes all appropriate phases and whether they were completed as prescribed by the plan.

c. The audit trails, exception reports, and system security designs are adequate.

d. The testing is adequate.

e. The adequacy of user manuals, terminal operating guides, and computer operator instructions.

f. The board, senior management, applicable committees, computer operations, user departments, and audit were involved in all phases of the development process and if such participation was consistent with the plan's review and approval requirements.

g. Based upon documentation, audit reports, committee minutes, memorandum and discussions, the project was successful in meeting the objectives established in the system's definition phase.

APPLICATION PROGRAM DEVELOPMENT

4. Review selected documentation for at least one in-house developed program. Trace the programs' development from the initial request through the post implementation review process, and determine:

   a. If all required documentation is present and sufficiently detailed to evidence full compliance with established programming standards.

   b. The applicability and adequacy of involvement by senior management, committees, computer operations, users, and audits.

   c. Whether the program meets the objectives of the original request, based test results and user feedback.

   For MIS initiated program requests:

   d. Whether standard program request procedures were followed.

   e. If a user department was affected, whether there was appropriate consultation between users and IS departments.

f. Whether appropriate documentation and training was provided to users and computer operations.

OPERATING SYSTEM MAINTENANCE

5. Obtain and review the operating system installation plan, the system generation report, the system log, and other system related activity reports, and determine if: (Review changes made to the operating systems and supporting system software to determine compliance with standards, including adequate internal controls.)

   a. All functional system options are consistent with the approved installation plan.

   b. The overall supervision by management over system programmer activities is adequate.

   c. Supervisory personnel have sufficient technical background to supervise system programmers' activity effectively.

   d. The adequacy of controls over:

      (1) New system installation.

      (2) Implementation of new releases.

      (3) In-house enhancements or tailoring.

      (4) Emergency fixes and other temporary modifications.

      (5) Documentation of changes.

      (6) System testing.

      (7) Management or supervisory approvals.

   e. Controls over data altering utilities, user exits, privileged instructions, and libraries are adequate.

   f. System logs and reports record adequately system programmer activity.

   g. Vendor technicians and outside consultants are subject to the same policies and controls as in-house staff.

PROGRAM MAINTENANCE

6. Review program changes for selected applications to determine compliance with standards and the adequacy of internal control, and determine:

   a. If the program change control procedures provide adequate guidelines to control the function.

   b. If change standards and procedures are adhered to.

   c. If documentation is complete and contains adequate explanations for the omission of any procedures required by the written standards.

   d. The adequacy of involvement of users, audit, and information systems management in the request and approval processes.

   For emergency program fixes and other temporary changes, determine if:

   e. Prescribed procedures are followed.

   f. Documentation is sufficiently detailed to explain the nature of the emergency change, the immediate action taken to address the problem, and subsequent actions to permanently correct the problem.

   g. Emergency changes are incorporated into the next production version of the program.

TESTING

7. Determine whether standards require that:

   a. Test plans explain the overall testing approach and expected results.

   b. The approach includes testing for illogical conditions, out of sequence data, and excess volume.

   c. The scope included all functions, programs, and interface systems, and all test discrepancies are adequately documented and resolved.

d. Users and audit participate in the development of test data and the actual testing phase.

e. All test plans and results are documented and retained.

Based on systems and application program reviews determine if:

f. All testing standards were adhered to.

g. Test documentation is sufficiently comprehensive to support test conclusions.

DOCUMENTATION

8. For the applications selected, determine if:

   a. Overall systems and program documentation adheres to standards.

   b. Documentation is complete and current.

   c. Adequate controls have been established to safeguard documentation.

IMPLEMENTATION

9. Review documentation generated from the implementation process and determine if:

   a. Controls ensure complete integrity of programs between the test and the production environments.

   b. Adequate supervisory review and approval precedes all implementation of program products.

   c. System level implementations are subject to the same controls as application level activity.

DATABASE MANAGEMENT SYSTEMS (DBMS)

10. For the application selected, obtain and review the relevant data base(s) documentation. Review the applicable authorization table to determine who is authorized to update or

otherwise alter indexes, tables, rows, and columns, and determine:

a. The adequacy of written standards and procedures govern all aspects of the function.

b. A database system administrator exists, who has overall responsibility for software installation, software maintenance, performance monitoring, administration of security, database design, and application development.

c. The DBMS function is separate from the systems and programming and operations functions.

d. Controls for changes to the data dictionary.

e. There is a separation of duties within the DBMS function which prevents one individual from controlling the entire operation.

f. Adequate security controls to govern the granting of access rights.

g. Adequate procedures covering database failure, emergency fixes, backup and disaster recovery.

h. The adequacy of controls over access to and usage of query languages and sensitive DBMS utilities.

SECURITY CONTROLS

11. Obtain copies of the security access and control files for the operating system, major third party systems products, and interactive programming facilities. Also, obtain a list of data altering utilities, user exits, user interface programs, and privileged commands. Using these documents determine:

    a. Whether the data security administration function is independent of systems and programming or if sufficient compensating

controls preclude absolute control over major aspects of the function by one person.

b. If all programmers have unique user-IDs and passwords.

c. If auto sign-ons are prohibited.

d. If management has identified and documented all privileged or sensitive programs and library products and if access is on an absolute need basis only.

e. If strict controls govern their use, development, and implementation, including supervisor approval, activity logging, and review procedures.

f. If details of all in-house and vendor exits, and programs designed to run in supervisor state or otherwise capable of by-passing security are provided to the system security administrator and the audit department.

g. If system access and levels of authority are consistent with the job functions.

h. Whether the authority granted under global security systems (RACF, ACF2, TOP SECRET, etc.) do not circumvent local interactive program facility controls.

i. If all changes to the system security software are approved by the system security administrator or advised thereof, and if details of the changes are provided to the audit department.

j. If interactive programming and security software provides an adequate audit trail to identify the programmer, the programs or utilities used, the files or programs accessed, and the nature of the access (change, delete, view, etc.).

k. The adequacy of segregation of duties for application programming, systems programming, computer operation, and system security functions.

l. If management periodically reviews the user authorization file for accounts with unnecessary privileges and whether the review is documented.

m. If physical or logical separation between the production and test environments are maintained.

n. Whether one programmer can develop an entire application system, or independently access, modify, and introduce a program into production.

o. The adequacy of controls over dial-up access.

BACKUP AND RECOVERY

12. Review disaster recovery plans, emergency procedures and other relevant documentation, to determine if: (Coordinate this work with examiner assigned to review Corporate Contingency Planning.)

    a. There are persons with sufficient training and experience to provide backup for the major systems and programming functions.

    b. Operations has a list of person to notify if an application requires immediate maintenance.

    c. Sufficient backup is maintained, including original programs, to ensure continued production should problems be encountered during the maintenance process.

    d. Detailed disaster recovery procedures have been developed and incorporated into the overall disaster recovery plan.

    e. Duplicates of the operating system are available both on and offsite.

    f. Duplicates of the productions programs are available both on and offsite.

    g. All program and system software changes are included in the backup.

h. Duplicates of interactive programming software and other documentation are needed to reestablish both the systems and the application programming functions available offsite.

VENDOR SOFTWARE/SUPPORT

13. Obtain and review copies of all vendor and consultant contracts and agreements, available financial statements, escrow agreements, and applicable written standards, and decide whether:

    a. Software purchase and selection standards require:

        (1) Clear definition of user requirements.

        (2) Clear definition of system requirements (equipment, interface, etc.).

        (3) Cost/benefit analysis.

        (4) Software support (in-house or vendor provided).

        (5) Financial condition of vendor.

        (6) Escrow agreements.

        (7) User documentation and training.

    b. The financial strength and technical expertise of the vendor give assurances that it is capable of providing adequate maintenance support to satisfy the current and future needs of financial institution customers..

    c. The vendor supplies source code or maintains a third party escrow for the benefit of the serviced institutions, and whether the source codes held by the third party are the latest version.

    d. If contract programmers are employed:

        (1) Written contracts are in effect and the adequacy of insurance coverage.

(2) Managements' evaluation of qualifications; the degree of reliance management places on contract programmers; and the level of supervision exercised over the contract programmers adequate.

(3) They are subject to the same policies and procedures as in-house staff.

UPDATING STANDARDS AND PROCEDURES

14. Review the procedures for updating the systems and programming standards manual are decide whether:

    a. Procedures require:

        (1) That one person is responsible for coordinating all updates.

        (2) Updates are appropriately numbered and dated.

        (3) Periodic reviews are conducted to verify older entries.

        (4) Periodic review and approval by management.

    b. Procedures are adhered to.

CONCLUSIONS

15. Review the results of work performed in this section and in sections for Planning, Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

16. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

b. Recommended corrective action for deficiencies cited.

c. Management's proposed actions for correcting deficiencies.

17. Assign a rating. (See Chapter 5 for additional information.)

18. Prepare an index of workpapers for this section of the workprogram.

19. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

20. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

1. Do application system design/development standards require:

   a. An SDLC phase structure that includes:

      (1) User request?

      (2) A feasibility study including cost benefit analysis?

      (3) Detail requirements definitions, based upon user department input?

      (4) General systems design?

      (5) Detail systems design?

      (6) Program development?

      (7) Predetermined progress checkpoints for review?

      (8) Unit testing?

      (9) Systems testing?

      (10) Manual(s) development?

      (11) User training?

      (12) Acceptance testing, with written user approval of the design, test, and final acceptance?

      (13) Conversion?

      (14) Production support?

      (15) Post implementation reviews?

   b. The detail design phase including:

      (1) A system narrative?

      (2) A system flowchart?

      (3) Record layouts?

      (4) Data element definitions?

      (5) Report layouts?

      (6) Screen formats?

      (7) Program specifications?

(8) Test plans?
(9) Project schedules?

c. The project feasibility study provide sufficient detail to justify in-house development of the system as opposed to purchase?

d. A formal request submitted or agreement approved by the head of the user or steering committee before undertaking the project?

e. The definition process include user input at all levels?

f. A statement of purpose and definitions formally presented and approved by the department or committee before actual coding begins?

g. The definition phase including:

(1) All programs or modules of the system and narrative about purpose?

(2) Sample forms and output reports?

(3) Detail security and other features?

h. The presence of all elements of the detail design phase?

i. That elements agree with the definition approved by the user?

j. That all elements been reviewed and approved by appropriate committees?

k. Pre-check intervals that are sufficiently spaced to allow for adjustment to production without disruption to the overall project?

l. Intervals sufficient to allow for a test of key modules?

m. All aspects of the system testing to use live backup data and prepare data designed to exceed acceptable parameters? (Note: Generally, extremely sensitive live data should not be used in the testing process.)

2. Do application programming standards require:

a. Full documentation including:

   (1) program narratives?
   (2) Logic diagrams?
   (3) Input records and descriptions?
   (4) Output record format and descriptions?
   (5) Master file formats and descriptions?
   (6) Source code listings?
   (7) Operating instructions?
   (8) Descriptions of test data?
   (9) User instructions, if applicable?

b. User involvement in major decisions affecting input, logic, flow, and output?

c. Embedded edit routines, including control totals, program edits, and validation checks of inputs before any processing is done?

d. Development of audit trails and exception reports of uncommon transactions?

e. Use of standardized programming languages, naming conventions restart routines, and modular code?

f. Systems programmers to be restricted in their access to application program libraries and documentation?

g. Application programmers be denied access to:

   (1) The computer room?

   (2) Operating system documentation and systems programming work areas?

   (3) Documentation and source codes for programs for which the programmer has no responsibility?

   (4) Documentation and source listings for the operating system?

   (5) Production program libraries?

(6) System level utility programs and other privileged programs and libraries?

(7) Live data files?

h. Procedures to change or remove access for programming personnel that leave the functions?

i. Procedures for terminated or suspected security risk employees?

If automated program development and control software is used:

j. Individual libraries for all programmers?

k. Programmers be restricted to his /her library? If not, is access to other program libraries read only?

l. That programmer sign-ons default to their libraries?

m. That programmers can't escape their libraries into the operating system environment?

3. Do operating systems activity standards include:

a. An overview of the system program function, including responsibilities and prohibited activities?

b. Specific instructions governing each defined task?

c. A detailed description of the operating system including:

(1) Implementation instructions?
(2) Security features?
(3) Description of utilities?
(4) Control or command language requirements?

(5) User error messages?
(6) Error detection and correction features?

(7) List of all files and modules used by the operating system?

d. Standards that require:

(1) Separation of the systems and application programming functions?

(2) Separation of computer operator and system programmer activities?

(3) Separation of the system security and system programming functions?

(4) Complete documentation of the system operating environment, including user enhancements?

(5) Changes to the operating system to adhere to formal change control procedures?

(6) Notification to the security administrator and audit departments of all programs designed to run in supervisor state or otherwise circumvent system security and logging controls prior to implementation?

(7) Identification, documentation, and control of privileged and other sensitive system level programs?

e. Access appropriate for the function performed?

f. Systems programmers be prohibited from accessing the computer's interior or the computer console, except under the supervision of computer operations personnel?

g. That the auditor and security officer maintain a record of all privileged programs, data altering utilities, and other sensitive code?

h. All elements are included in the system generation approved by management?

i. Complete documentation is maintained for all operating systems?

j. A record of all user interfaces, exits, and routines properly documented?

k. Automated logs that produce detailed:

(1) Operating system accesses?
(2) Utility accesses?
(3) Network accesses?
(4) System halts and restarts?
(5) Software modifications?
(6) Accesses to the system clock?

l. That logs be reviewed by supervisory personnel for any unusual activity?

m Whether automated logs can be turned off by unauthorized users?

n. If the logs are retained per a retention schedule?

4. Do program change standards require:

a. Management review to determine feasibility and appropriateness of changes?

b. Testing procedures?

c. User approval prior to implementing changes?

d. Chronology of program changes?

e. Preprinted forms and procedures for requesting program changes, including:

(1) Pre-numbered program change control forms?

(2) A description of the problem or reason for the change?

(3) Approval of the change request by the affected user department?

(4) Names of the programmer making the change?

(5) Signatures of another programmer or supervisor who reviewed and approved the actual program change?

(6) Signatures of the program librarian or quality assurance personnel cataloging the program changes?

(7) Forwarding a copy of the approval to the audit department?

f. Supporting documents, e.g., source listings of codes affected by a change, JCL check listing, and the directory listing of the source and object library?

g. Program modifications be reviewed and approved by the user department prior to implementation?

h. Program documentation be updated to reflect program changes as soon as practical?

i. Temporary program changes be replaced by properly authorized source program changes as soon as practical?

j. Change requests adhere to standards?

k. Change request numbers cross reference all other related documentation?

l. The program modification be tested before installation?

m. Both the program and system documentation be updated to reflect the change?

5. Do documentation standards and procedures require:

a. A formal program documentation librarian function or a person to control documentation?

b. A function independent of other responsibilities that may conflict with documentation control activities?

c. Written policies and procedures governing the function's activities?

d. That documentation librarians' duties include:

(1) Review of documentation during system development to ensure adherence to standards and appropriate authorization of exceptions?

(2) Control and safeguard of documentation?

(3) Revision of documentation to reflect the changes?

(4) Distribution of documentation to authorized parties?

(5) Periodic inventory to account for documentation?

(6) Maintenance of all documentation and standard's manuals to ensure that they are kept current?

(7) Assurance that documentation is adequately backed up offsite.

e. That the librarian control:

(1) All vendor documentation?

(2) All systems documentation?

(3) All application program documentation?

f. That vendors' Technical Engineer's (TEs) documentation is not controlled by the librarian, and that adequate controls have been established to prevent unauthorized access?

g. The librarian function to be available for all shifts? If not, have adequate controls been established for retrieving documentation?

h. That documentation be housed in a physically secure environment?

i. That the environment be protected by fire suppression devices?

6. Do database administration standards require:

a. An administrator to be assigned the responsibility of coordinating and controlling the use of all data bases?

b. The administrator to be independent of the systems programming function?

c. The administrator to establish standards that control overall DBMS activity and include:

   (1) defining the database elements?

   (2) Maintenance of the data dictionary?

   (3) Database design?

   (4) Database operations?

   (5) Security?

d. The administrator's access to live data, application source listings, and other application program documentation be adequately restricted?

e. Subadmistrators to be designated and their authority and activities appropriate and adequately controlled?

f. Access to sensitive DBMS program utilities and high level administrative privileges. Appropriate and regularly monitored?

g. Detailed definitions of data items in a data dictionary or central catalog?

h. That changes to the dictionary be:

   (1) Authorized through the data base administrator?

   (2) Approved by users where applicable?

   (3) Amended in user documentation?

   (4) Adequately tested?

   (5) Reviewed for audit trails and controls?

i. That procedures are in place to ensure that the data dictionary remains current and accurate?

j. The data base administrator have a list of all exit routines that interface the DBMS?

k. The administrator to approve all exits developed in-house?

l. The administrator approve all in-house programs that access the data base?

m. Procedures provide for the prompt notification of users of all changes affecting them?

n. Procedures to cover data base recovery in the event of hardware or software failure?

o. Procedures include periodic dumps of critical data during the processing day?

p. Adequate disaster recovery considerations have been documented and tested?

q. A transaction log provides an audit trail of entries?

r. The log indicates attempts to violate DBMS security?

s. Activity reports and exception reports are reviewed daily?

7. Proceed to procedure 15, Tier I.

Examiner | Date

_____|_____

Reviewer's Initials

OPERATIONS CHAPTER 13

(FILE NAME ON DISK # 1 = S2C13.WPD)

The computer operations department is responsible for selecting, operating and maintaining computer and telecommunications equipment that retain and process information assets of the institution. The department must maintain a stable production environment, process the data promptly and efficiently, and protect the data files, programs, and equipment under its control.

The computer operations department generally has responsibility for the following functions:

- Computer operations.
- Communications network control.
- Data preparation.
- Transaction processing.
- Workload scheduling.
- Media library.
- Documentation library.
- Performance monitoring.
- Disaster contingency planning.

The controls described in this section generally describe centralized computer facilities. However, the concepts also apply to end-user computing systems located throughout the organization.

In order to perform their job functions, computer operations personnel must have access to the information necessary to run various equipment and programs. All information for processing work should appear in the Operator's Run Manuals. The information should be limited to the functions to be performed, the hardware, software and data files to be used for processing, and maintenance of the equipment. Run manuals normally include processing procedures, rerun instructions, special application instructions, file rotation procedures, recovery instructions, and emergency procedures. Computer operators should not have access to software or hardware documentation that is not necessary to perform their duties. Management, assisted by computer operations and systems development and programming personnel, must ensure that Operator's Run manuals are current.

There also should be an overall procedures manual for all computer operations functions. This manual should cover matters, such as equipment maintenance, equipment operation, staff policies, and coordination with other departments.

Just as computer operators must have sufficient instructions to run the system, users must have the necessary information to properly use applications. User manuals providing information on the preparation and control of source documents, along with the control, use, and format of output should be readily available. The user manual should include examples of documents and sufficient details about the reconcilement of applications.

SEPARATION AND ROTATION OF DUTIES

Operations management must implement policies and procedures for separating and rotating duties, and cross-training personnel. The size of the installation will influence the types of policies implemented for the division of duties.

Separation of duties is a basic internal control procedure. Management must assign duties to separate responsibility for different elements of computer operations and application processing. Computer operators should not perform any duties other than those directly relating to equipment operation. However, this is not meant to prohibit operators from learning other duties or from performing them in an emergency. For example, there should be no overlap between computer operations and data preparation for processing. Generally, computer operators should not perform duties such as reject re-entry, general ledger balancing, or unposted items settlement. No one should be permitted to perform one function from start to finish or be responsible for checking the accuracy of his or her own work. In all areas of the financial institution, separation of duties is the best deterrent against employee dishonesty or intentional harm to equipment, documentation, or records. If this control is present, a person wishing to subvert the

system is forced into collusion with other personnel.

Rotation of duties serves as both an internal control and cross-training tool. Tasks and shifts should be rotated among computer operators to: provide each operator with training for operational tasks, and prevent operators from handling any one function indefinitely. Rotation of employees should be of sufficient duration to permit disclosure of any irregularities. The implementation of rotation assignments, in large measure, depends on the size of the installation.

In smaller institutions, where there is little separation of duties, rotating duties takes on added significance as an internal control measure. The actual rotation should be logged to document performance. When people normally not responsible for running the computer act as operators, computer time must be closely controlled, and continual management review of the conflicting functions is necessary. As in other departments, mandatory vacations for at least two consecutive weeks should be encouraged for all IS personnel.

In large centers with separation of duties, the possibility of an individual jeopardizing the integrity of the institution's information systems is minimized and rotation of duties is less important as an internal control. However, in such instances, rotation provides effective cross-training and should be used whenever possible.

EQUIPMENT MAINTENANCE

Preventive maintenance on equipment should be performed at all installations. This includes minor maintenance, such as cleaning peripheral equipment by center employees, as well as more extensive maintenance provided by the manufacturer or vendor. Computer operators should not be permitted to repair equipment or perform other than the most routine maintenance.

Maintenance by computer operators should be performed according to manufacturers' recommendations. As a general rule, these duties include:

- Cleaning tape heads each shift.
- Cleaning printers daily.
- Checking and cleaning the MICR reader/sorter at the end of each shift.
- Periodically checking and cleaning the area under raised flooring.

Maintenance schedules may vary considerably depending on the size of the installation and the volume of work processed. All maintenance should be performed according to a predetermined schedule, not on a random basis, and recorded in logs or other records. Management review of these records could aid in monitoring employee and vendor performance.

Maintenance by the manufacturer or vendor usually will be performed under contract. If equipment is leased from the manufacturer, the maintenance agreement may be part of the lease. When equipment is owned or leased from a third party, a separate maintenance/service agreement between the IS department and the equipment manufacturer should be used.

The service and maintenance agreement should provide repair services, detail the preventive maintenance to be performed, and indicate a schedule for both. When a center uses hardware from more than one manufacturer, maintenance boundaries should be defined. Under such conditions, it may be desirable to enter into an arrangement whereby one vendor takes responsibility for seeing that overall repair maintenance is accomplished. Under this arrangement, whenever hardware problems are encountered, the data center would contact the designated vendor to determine the source of the problem and to assure that vendor makes the necessary repairs. In any event, data center management should ensure that maintenance contracts guarantee timely performance.

A certain amount of computer time should be scheduled for preventive maintenance. During this maintenance, the service representative (computer engineer or customer engineer) will service the equipment, e.g., change filters, fill oil reservoirs, and check all indicator lights, hardware circuits, and other mechanisms. When this occurs, the computer operators should dismount all program and data files and work packs, leaving only the minimum software

required for the specific maintenance task on the system. If this is impractical, appropriate systems activity logs must be reviewed by operations management to check security regarding access to programs during maintenance. Also, at least one computer operator should be present at all times when the service representative is in the computer room.

Operators should maintain a written log of all hardware problems and downtime encountered between maintenance sessions. A periodic report on the nature and frequency of those problems is a necessary management tool, and may be valuable for vendor selection, equipment benchmarking, replacement decisions, or planning increased equipment capacity.

EQUIPMENT OPERATIONS

Operation of the computer and its peripheral devices is best accomplished by following manufacturers' procedures and operator instructions. Manuals for equipment operation should be current, describing the computer system actually in use, and be readily available to computer operators.

Operator's instructions should include:

- Identification of all input/output forms (including samples of special forms).
- Instructions for forms alignment.
- Explanation of the run purpose.
- Detailed instructions for the disposition of input and output.
- Identification of all programmed halts and operator responses.
- Prescribed start and restart instructions.
- Description of records used and hardware requirements.
- Run frequency and priority.
- Sequence in which programs are to be executed.
- Description of all special instructions or conditions.

An operating log or file should be maintained to record any significant events and actions taken by computer operators. This usually would be prepared by the lead operator of each shift and inspected daily by operations management to ensure that operators are following instructions. IS management should restrict the use of computer equipment and media, and the actions of operators and other personnel whose duties affect the operation. These restrictions should be in written operating procedures. The procedures should be current and sufficiently detailed to guide operation of the computer center.

SCHEDULING

Computer workload scheduling is critical to efficient IS operations. Many data centers use automated scheduling programs. Applications run on large or highly sophisticated computer systems usually cannot be scheduled effectively without reliance on automated programs. Regardless of the complexity of the scheduling procedure, certain questions must be considered in all installations:

- Does the schedule make efficient use of computer resources? All users want their jobs run early to ensure prompt delivery. However, an efficiently operated center does not schedule production runs and produce reports for all applications during the prime processing shift, leaving the computer system idle for the remainder of the day. Neither does it schedule jobs to run so early that the provider of the input cannot be ready, or so late that the output will be delivered later than needed.
- Does the scheduling procedure take into consideration the late arrival of input? The schedule should contain cutoff times after which the job must be run with only available input or deferred until a later time. No job should be delayed indefinitely, thus holding up all others set to run after it. In certain cases, running an application with incomplete data may be inefficient; in other cases, it may be appropriate to run the application with available data only.
- Are all jobs assigned an overall priority rating? Priority ratings should be assigned to all jobs run on a regular basis so that critical applications will

be run first, after recovery from an emergency. For example, if such a priority system is not used, and there is a hardware failure (which can hold up processing for several hours), critical applications such as deposit applications, may be in the queue awaiting execution when the financial institution opens on the following day.

Non-routine computer runs should be supported by a work request or other written authorization. This includes all unscheduled production jobs, assemblies, compiles, and tests. All scheduling should include due-in/due-out times and dates of input and output; records covering delays in receipt of input, data processing and delivery of output; and adherence to priorities. Schedules, whether manual or computer prepared, should be compared against actual run times.

System usage reports indicating scheduled and unscheduled production time, program test and assembly time, reruns and maintenance periodically should be prepared. They should be reviewed by installation management, and variations from scheduled activity should be investigated. Additionally, the backlog of jobs awaiting processing by each shift should be reviewed for reasonableness.

BACKUP

The creation and rotation of backup tapes is a vital function of the operations area. Adequate onsite and offsite backup of operating systems, application programs, master data files, and transaction files is essential as processing systems are susceptible to many types of disruptions. Disruptions can be caused by system crashes, equipment problems, program or data file corruption, physical, environmental, or other types of site related disasters as discussed in Chapter 10. The lack of timely and comprehensive backup procedures may lead to significant expenses in reconstructing programs or data files, and could lead to operational failure. Backup files should be rotated offsite as soon as practical after creation to reduce an institution's risk exposure.

Program File Backup

Program files generally consist of the operating system and application programs. In less complex systems these files will be located in a few libraries/directories and can easily be backed up by copying entire libraries to tape. More complex systems maintain many of libraries/directories and may require automated library systems to manage the backup process. Operations management periodically should review programs and the contents of program libraries/directories to ensure backup procedures are adequate. In more complex organizations, this review likely will require user input into the function and importance of files in their libraries.

At a minimum, program file backup should include:

- The current operating system.
- The object code version of production application programs.
- Source code files for production programs. (If programs are supported in-house)
- System utilities which are utilized by operations. (Includes text editors, compilers, etc. if programs are supported in-house)
- Any other programs which are necessary to restore operations at the recovery site.
- Documentation for all of the above.

This list provides a bare minimum of the program files needed to operate the computer as a snapshot of its current configuration. Many institutions also routinely backup source code program files, files in programming development libraries, files in programming test libraries, and other files as deemed appropriate. Backup tapes of program files should be created after every system update.

Master File and Transaction File Backup

Master files and transaction files requiring daily duplication and rotation off premises will vary. In any case, master files and transaction files sufficient to recreate the current day's master files must be stored both on and off premises, as backup for each application processed. For applications that do not produce a daily master file, a cumulative transaction journal should be used and backed up in the same manner as master files.

In a distributed data processing environment (LANs), disk mirroring and/or disk duplexing provides real time backup of data to a secondary disk, so that it can

be used should the primary disk become nonfunctional. With mirroring, data and operations can continue immediately without any disruption to the user. Regardless of whether the LAN has disk mirroring and/or duplexing, institutions that process data on a LAN should store regular periodic backups of the programs and data offsite, using a similar retention methodology as with mainframe data (indicated above).

Because computer systems differ, the vendor should be asked for the most suitable backup rotation plan. If the only backup copy of files are stored in the computer area, a fire, or other disaster could destroy all machine-readable records. In that case, the institution would either be unable to create a current master file or have to recreate a machine-readable file from all available source documents. The latter option is expensive and time consuming. To avoid this situation, the financial institution should store a current copy of the master file and subsequent transaction files at a remote location. The remote location can be a fireproof box at a local business, another financial institution, a branch office or, as a last resort, at an employee's home. Although the location should be relatively secure, having data stored offsite even in a nonfireproof location is more desirable than no off-site storage, because simultaneous destruction is less likely. The key is that it must not be a site that is subject to the same disaster.

Some institutions will store all backup files in the main vault. Although this reduces risk and may be appropriate for paper documents with high heat tolerance, it is not the most desirable since off-site storage is almost as easy to implement and provides significantly more protection. If the computer facility is completely destroyed, the financial institution should be able to resume normal processing as soon as alternate equipment is available provided backup files are stored off-site.

Procedures relating to file retention and offsite-storage should normally require:

- Maintaining off-premises backup files in machine-readable form.
- Reducing the lag, and the potential exposure, between the creation of current master file backups and the rotation of these files to off-premises storage.
- Rotating new backup files to off-premises storage before returning old backup files to the data center.
- Keeping off-premises storage sites environmentally controlled and physically secure.

Procedures relating to the use of backup for data files and program libraries, whether in-house or remote, normally include:

- Recopying backup files prior to use.
- Copying a file before it leaves the data center to provide in-house backup.
- Logging out a file when it is removed from the file library or off premises storage (time, date, and method of replacement also should be noted).

Where a backup copy of the newly created master file cannot be quickly removed from the data center, copies of pre-processing transaction files should be removed from the site. This would ensure the ability to recreate a master file with current information.

EQUIPMENT CONTROLS

Equipment controls refer to procedures that prevent or detect unauthorized program execution and computer usage. These controls are usually more effective in detecting when and how unauthorized use occurred rather than in preventing it.

Equipment controls basically consist of the console printer, internal CPU clock, and system activity logs. The console printer indicates communication between the operator and the machine. The internal CPU clock allows the computer to show a time for each job initiated. Console printer paper should be retained intact after each day's processing for management or audit review.

Operator console activity may be stored on disk or tape and exception items extracted for management and audit review. Console logs are a valuable management tool and audit trail which should be used properly by operators.

System activity logs are files created and maintained by the supervisor program. System activity logs record communication between the computer and the operator, and between different parts of the computer system. They cannot be suppressed by the operator if the operating system is properly restricted. The logs are maintained on disk or tape and should be

printed periodically for management and audit review.
Job accounting software or audit retrieval software is used often to summarize a large volume of data. Detailed system usage reports can be developed, and the detail provides an excellent audit trail. A summarized version of such data is appropriate for periodic reports to senior management for all but the smallest installations.

Even the most sophisticated equipment control will lose much of its effectiveness if proper operating procedures are not instituted and maintained. As with nearly all other areas of IS, procedures may range from basic to sophisticated. In all instances, certain minimum procedures should be in effect, including:

- The computer room should not be left unattended while the computer system is in operation. This will help prevent unauthorized use of the equipment as well as save valuable time in the event of a system problem or emergency situation.

- At least two computer operators should be assigned to each shift where practicable. This ensures that one operator will not be able to do any unauthorized work and provides personnel backup.

- Operators must not be allowed to unilaterally override any hardware or operation system checks. This refers to internal label checks, read/write checks, etc., and minimizes the likelihood of processing the wrong data or destroying live data.

- Operators should be required to run all jobs according to the schedule to prevent unauthorized jobs from being run.

- Operators should not allow non-authorized personnel to run the equipment. This applies to all persons who are not console or equipment operators. It will guard against unauthorized use of the computer, especially for systems or applications programmers whose control may be excessive if allowed access to computer operations.

OPERATOR CONTROLS

Computer operators generally have access to programs and data on the system through the equipment and may exercise latitude (equal to the flexibility of the hardware and software environment) in dealing with day-to-day processing. To establish an adequate level of security and internal control, specific rules should be written to limit the scope of and properly direct operator activity.

Rules common to most computer centers are:

- Operators should not execute data or software-altering utility programs without proper authorization. Such programs should be either removed from the system and placed under separate control or maintained under the password protection of an automated library routine (see Chapter 12).

- Operators should not have access to source programs or program listings. Access to other documentation not required for the processing of applications also should be restricted. This will help prevent operators with programming knowledge from making unauthorized changes to production programs.

- Operators should not perform any balancing functions other than run-to-run controls.

- Operators must observe all security procedures including proper library procedures. This will prevent unauthorized access to the equipment, data files and program libraries.

- Operators should initiate the execution of only those programs submitted in accordance with established data center procedures.

LIBRARY CONTROLS

Library controls are procedures to maintain, and prevent unauthorized access to data files, programs, and documentation. There are several libraries in any computer installation. A physical library exists for data and program files, whether they are on magnetic disk or tape. This library should be a secure room area where files can be stored adjacent to the computer room to facilitate the retrieval and storage of processing files. A physical library also exists for system and program documentation, generally in the systems and programming area (see Chapter 12 for additional information). Operator access to systems and programming documentation should be restricted

In addition to physical libraries, several types of

program and file libraries are usually part of the computer system. Program libraries consist basically of three types: test, production and private. A test library contains those programs or modules currently being modified or developed by the programming staff. Production libraries contain programs used to process the center's work. Private libraries are sometimes used to retain software that does not conveniently fit the other two categories. The existence and use of private libraries should be addressed in installation standards and be closely monitored by operations management. For each of these program libraries, both a source version and an object version of the library are generally maintained.

Lacking any restrictions, an operator can read, copy, execute, rename, delete or replace a program from the computer system libraries. Since these program library maintenance functions should be restricted, many installations use a library software package for program library control. Some packages are RACF, LIBRARIAN, SECURE, PANVALET, and PANEXEC. Such packages are available through equipment vendors and commercial software firms. In addition, some installations have developed their own library routines. Regardless of the package, library software usually performs a combination of the following functions:

- Restricts access to source (and possibly object) programs on an hierarchical basis, often using a key or password which denotes the authority level of an individual user. For instance, operators might be restricted from access to the test and production library source versions, but allowed access to production library object versions. Restricted library maintenance functions might be reserved for the shift or operations supervisor. When on-line interactive programming is practiced, programmers might be authorized to change test libraries, but not production libraries. Further restrictions could be imposed by application, according to assigned responsibility for programmer maintenance of an application.

- Maintains on a separate file the date and time of access, type of operation performed (such as execute, copy, rename, and read), and identity of the individual (or program) which accessed the module.

- Provides periodic printed reports of the previous information, and:

  - The date last changed or renamed.

  - The version number.

  - The number of times executed or accessed since previous report.

  - The program's status, e.g, test, production, active, inactive.

The control, recording and reporting capabilities of library software vary. Occasionally, such software is adapted to control access to data files in the same manner. In those instances, the proper password often is in the updating object program. When passwords are used, they should be changed periodically and suppressed or made illegible on output.

A second type of software associated with data file libraries is the automated data file inventory. Although a manual inventory of data files can be satisfactory, many installations automate the process of listing the physical location of a file. Although useful, such a system should not be confused with library control software because the function differs substantially.

Some basic considerations for controlling access to files and libraries in all installations are:

- Assigning specific responsibility for the maintenance of production libraries. This will help prevent storing different versions of a program in both the source library and object library. In addition, this function should ensure that source programs supporting each object module are in the library and that all obsolete modules are promptly removed.

- Providing proper authorization to operations personnel to support any changes to production libraries. This requirement is essential for preventing unauthorized changes. The audit trail thus created should be easily traceable to the program change/project request approval mechanism existing in the systems and programming department.

- Denying operators access to magnetic media other than those required for processing application. Although this requirement may not be feasible in

smaller operations, it is essential in centers using a significant number of magnetic files. Without it, accurate inventory controls of those files cannot be maintained. In addition, it will minimize the possibility of processing the wrong file or destroying live files.

- Prohibiting operators from executing programs from test libraries during production runs. Permitting this will circumvent most controls included in the procedure for placing programs into a production status. This procedure, known as cataloging, would include such controls as: (1) requiring proper authorization for placing a new version of a program into the production library, (2) verifying that the program has been adequately tested, and (3) requiring that program documentation has been developed or updated.

Controls over access to on-line program files also are discussed in Chapter 12, Systems Development and Programming (Program Security), and in Chapter 14, Security Physical and Data (Program Security).

CONTROL OF DATA FILE MEDIA

Computer-based records (disks, tapes, drums, or cells) are critical to the operation of an institution. Care must be taken on all computing systems when storing various media to ensure adequate protection against physical hazards.

Air-conditioning and humidifying equipment should be used to maintain suitable temperature and humidity levels for stored media. Consideration also must be given to the media's susceptibility to destruction by electromagnetic field radiation from generators, radar installations or other power sources located nearby. For many computers, especially smaller systems, such as minicomputers, microcomputers and LANs, the files are retained on the computer's fixed disk at all times. The loss of these files without proper backup could cause disruption of business operations and a significant investment of effort to recreate the files from manual records.

Damage or loss of media through fire and other disasters is an important control consideration. Even though a fire may occur in an area adjacent to the media storage room or elsewhere in the building, the resulting heat could destroy data recorded on tapes, disks and similar media. In addition, water used by fire department personnel in combating fire may cause extensive damage to media.

Physical security and control procedures for current and backup data must be as effective as preventive measures installed to protect media against environmental disasters. Ideally, all on-site data files and scratch tapes are stored in a separate room adjacent to the computer equipment. Access to that room should be limited to authorized personnel (normally data file librarians and, in emergencies, shift supervisors). Tapes and disks should remain in this room, i.e., library, unless they are needed for production, are destined for off-site storage, or there is advance management authorization for removal.

If emergency access to the library is required, written procedures should provide that a record is made and reviewed by installation management as soon as possible.

The most desirable location for housing backup is in a separate building away from the data center so that a disaster occurring at one location likely would not affect both sites. However, remote (or offsite) backup should be readily accessible in the event on-premises files become impaired. The same environmental and security considerations must be observed for backup files as for those in the data center library. In addition, sign-in and sign-out records should be maintained, and there should be dual control access procedures at the remote storage location. If management maintains that on-site backup provides adequate protection, the board of directors should review and approve this procedure with its associated risks.

In data centers where only one tape librarian is employed or the position is part-time, controls over access to the tapes and disks are as important as they are in larger data centers. Control may be achieved by locking all data files in a fire resistant vault and by using dual custody procedures to remove files from the vault. If the vault does not have two separate combination locks, the numbers used for the combination can be split between two people. Care must be taken in selecting these persons. The effectiveness of the desired controls could be compromised if both parts of the combination were

given to two persons performing the same function. Procedures may be established to allow a shift supervisor emergency access to the tape/disk library in the absence of the librarian. These access procedures should be recorded and reviewed by management.

Tape and disk library procedures should encompass:

- Automated tape library systems or manual procedures in use.
- The daily housekeeping requirements.
- Accountability for newly purchased tapes and disks and retiring old or worn media from active use.
- Periodic inventories of all tapes and disks.
- Retention check and retention schedule for application and program data maintained on tapes or disks.

In all cases, media stored in magnetic form must be protected from loss and unauthorized access. Management should view any compromise of effective control procedures as a possible source of financial loss. Such risk is possible whenever an employee either intentionally or unintentionally – supplies confidential customer information to unauthorized parties. This could result in the financial institution losing business and customer confidence, and being subject to legal action.

A simple but effective method of protecting data on magnetic tape is the file protect ring (read/write ring) which, when inserted in the tape reel, allows information to be recorded. When the ring is removed, information recorded on the tape cannot be overwritten.

This feature may work in reverse on some equipment, but the concept remains the same. Some installations may leave the file protect rings in the tape reels at all times and use an automated tape library management system to determine when a tape may be overwritten.

Disk files can be protected by software controls. One such control is called a file protect feature. This control is a label checking routine that, upon opening a file, compares the creation date, volume number, data set name, and scratch date against the information contained in the program or job control cards. Any discrepancies, such as unexpired scratch date, wrong volume number, or data set name, will be displayed on the console. If an override is intended, the operator must respond through the console. All operator overrides should be logged and be subject to supervisory approval and review.

Some data centers have installed data and program file management systems that help preclude accidental destruction by operator error. However, these systems can be intentionally compromised or bypassed by knowledgeable operators.

The best procedural control is to use external and internal labels. External labels enable operators, tape and disk handlers, and librarians to easily identify the correct tape or disk. In some data centers, color coded tape reels or disk covers are used to distinguish files.

Where descriptive labels are used, any written procedures should be reviewed and compared to actual practices and hard copy records, such as the tape history card. File creation and expiration dates also should be compared to retention schedules. In most data centers using external label identification, the absence of a label indicates that the tape or disk has been released for reuse (scratched).

Many installations using automated librarian systems require only the serial number of the tape or disk to be displayed on the external label. Contents of each tape or disk can be determined by referencing the automated library system reports or by interrogating the library control system via terminals.

Internal labels reduce the possibility that an incorrect tape or disk will be used. However, an operator can often override internal labels. Operators should be informed, in run instructions and verbally, not to override internal labels without prior supervisory approval.

When used, internal labels are located at the beginning and end of data on the file. The header label generally contains the name of the file, the creation date, a volume serial number, a reel sequence number and, in some cases, the date the file expires. The trailer label may contain a record count of the number of records or blocks of information between the header label and the trailer label. It may also provide control totals and information signaling the end of the file or reel. Internal labels should be standardized throughout all applications,

subprograms, test files, master files and transaction data files. The use of nonstandard labels may force computer operators to override labels from time to time, diminishing the effectiveness of this control and increasing the possibility of accidental destruction of data and program files. In addition, the efficiency of production jobs may be reduced because nonstandard labels require manual intervention.

Once data and programs are contained in the computer's memory, boundary or storage protection can prevent the data and programs from entering areas of memory designated for other data records and programs.

HOUSEKEEPING

The computer operations personnel must maintain a clean, neat and orderly working environment. Cleanliness in the computer room and surrounding areas decreases the possibility of fire and damage to the computer and peripheral equipment. This is accomplished by:

- Preventing the accumulation of trash in or near the computer room.
- Dumping waste baskets outside the facility to reduce dust discharge.
- Shredding, or otherwise controlling before disposal, waste material containing confidential information.
- Prohibiting eating, drinking, and smoking in the computer room to prevent spills and ashes from damaging equipment.
- Limiting the supply of paper, forms, magnetic media, and other combustible materials located in the machine room(s) to the amount necessary to complete one day's work.
- Maintaining excess forms and supplies in a fire-resistant storage area outside the computer room.
- Permitting only small quantities of cleaning fluids, such as those used to clean tape drives, in the computer room. In general, flammable liquids should be stored away from the computer room and paper storage areas.

EMERGENCY PROCEDURES

Steps to be followed during and immediately after an emergency should be well documented. Since it is not safe to assume that security procedures will prevent the occurrence of an emergency, they must be developed to address such threats as fires, floods, sabotage, riots, bomb threats and acts of nature in proportion to their relative risk of occurrence.

Emergency procedures should personnel and property during emergencies. Instructions for shutting off utilities, powering down computers, protecting data files and documents, activating fire extinguishing systems and other fire fighting equipment, personnel evacuation, and securing valuable assets should be detailed for each area of responsibility, e.g., computer operations, programming, input/output, and end-user processing. The emergency procedures also should provide restart and recovery procedures.

The procedures should be posted conspicuously throughout the organization with implementation responsibility delegated to specific individuals. This reduces the possibility of equipment damage and minimizes the risk for the data center as well as the remaining employees who depend upon computer equipment. Periodic fire and emergency evacuation drills should be conducted and feedback from employees should be encouraged to assess the feasibility of the plan.

TRANSACTION PROCESSING

Financial institutions must receive, record, and process customer transactions in an accurate, reliable, and timely manner. The integrity, reliability, and accuracy of data depends on the establishment of proper control procedures throughout all phases of transaction processing. Whether the control procedures are manual, automated or a combination, coverage should include transaction initiation, data entry, computer processing, and distribution of output reports. These control considerations apply to new technologies such as truncation of items, the electronic presentation of checks, and electronic return items.

The control procedures relating to transaction processing discussed below are neither all inclusive nor recommended for all situations. Each processing environment must be evaluated individually to determine if data integrity is maintained throughout the transaction cycle.

Transaction Controls

The following are important internal, transaction control considerations:

- Duties must be segregated and management supervision should oversee transaction input processing and output functions.
- Overnight control of dollar totals for rejects and holdover items must be well defined and effective.
- Work returned from processing must be reconciled and balanced to the previously established control totals.
- Exception items must be cleared in an expeditious manner (exceptions are contrary to effective control and create potential risk to the financial institution).
- Exception reports must be reviewed by key officers and operation supervisors.
- All output must be produced, properly distributed, and controlled.

Complete control must be maintained over all input documents received at the data center. Input received from one user may need to be separated from that of other users. An effective control over batches of work is recording the batch number and corresponding batch dollar total on a standardized form when the work is initially received at the data center. A separate form should be used for each user.

The department receiving the daily work from users may have a variety of duties, depending on the size of the data center operation. In large installations, the receiving department clerks may spend an entire shift combining batches of work into blocks for capture. In small installations, the receiving clerks may receive the work, log it in, combine batches to make blocks, capture the data through MICR reader/sorters, reconcile the processed work, and collect all entries and reports for return to the users. This is a breach of segregation of duties and should be avoided. Although receiving clerks may accept work for set up and capture and receive entries and reports after reconcilement for return to users, they should not capture or reconcile the work as an additional duty.

Generally, segregation of duties must be achieved so that an individual is not responsible for any two of the following functions:

- Input preparation.
- Operating data input equipment.
- Operating computer and sorting equipment.
- Preparing rejects and nonreads for re-entry.
- Reconciling output.
- Distributing output.

Management must always consider segregation of duties in identifying the desired controls in any size data center operation. Computer operators' duties should be restricted to the operation of the computer, i.e., they should not perform any balancing function. If this is not possible, other duties should be confined only to secondary functions. Segregation of duties becomes increasingly important in an automated environment because critical functions are concentrated in fewer hands.

TRANSACTION INITIATION AND DATA ENTRY

Transaction processing systems convert data from source documents, checks and customer transaction tickets to machine readable form. Three common methods of capturing source document data for information systems are: item capture using magnetic ink character recognition (MICR) equipment, item capture using optical character recognition, and terminal entry.

Item MICR Capture

MICR encoded documents are generally pre-encoded with account number and other transaction information, except for the dollar amounts, to nationwide standards accepted by all financial institutions using data processing equipment. The encoding of dollar amounts is usually performed on proof machines with built-in balancing features during the processing cycle. In some cases, as in the case of installment and mortgage loan coupons, the dollar amount is pre-encoded.

One method of establishing control in item MICR

capture is to limit the size of each batch of entries for data processing to no more than 150-300 items. When looking for differences, small batches are easier to handle and reconcile by user personnel and the data center clerks.

Proof Operations

The teller work, and work from other departments is bundled in batches with a batch ticket showing the dollar total of all the items in the batch. At the item processing center or prior to receipt, transactions are processed through a proof operation where the teller work is MICR encoded, proved, and balanced. Batches are consolidated into blocks and block tickets prepared for the total of all batches in the block. The trays of block work are passed to a high speed reader sorter where the MICR information on the checks and transactions tickets is captured by the computer for processing. The transaction tickets and checks are sorted during this activity. At the end of the workday, all the financial and application system item capture report totals are balanced and reconciled to the appropriate applications.

The total dollar amounts of batches submitted for daily processing should always be listed on a transmittal form from departments submitting the work. The transmittal form provides a total of batch debits and credits for each application. This control feature furnishes an audit trail for reconcilement to the general ledger and gives personnel dollar totals to balance the item processing capture runs. User departments and the proof areas should develop control totals since these amounts form the basis for all internal accounting controls i.e., subsequent run-to-run totals and final output records. This principle of internal control is equally applicable to all methods of data entry, whether MICR, key-to-disk or key-to-tape.

In small branches and departments lacking proof equipment, tellers or other branch personnel may prepare batches of checks, deposits, payments, etc., by running adding machine listings of dollar amounts, to develop batch control totals.

In offices and departments with multipocket proof machine equipment, these steps usually are performed:

- A proof machine operator enters the total for each credit and offsetting debit into the machine which encodes the item and sorts credits and debits to selected pockets.

- The dollar amount for each credit and debit entered is accumulated on a separate tape listing for each pocket to which the entries are sorted.

- Periodically the entries are extracted from each pocket and a total is taken for entries run to that pocket.

- Entries are bundled to make a batch with the tape listing from the pocket.

- A batch header is made, indicating the total dollar amount of the batch. Batches are accumulated throughout the day in this manner. At the end of the day, grand totals are taken for each pocket in the machine. These totals represent the control totals for all work processed that day.

Some financial institutions set up regional proof centers to reduce operating costs. These centers operate in a manner similar to the proof department of a single branch, but perform the proof operation for many offices.

In small branches, large branches or unit offices, the teller receiving the entries may prepare the manual batch. However, a second person should check the batches and prepare control totals for all batches on the transmittal form. In branches with proof equipment, tellers should not be permitted to run the proof machine. In financial institutions with multipocket proof machines, operators prepare the batches of work for the day and a supervisor checks the batch totals and control totals prior to the work being shipped for processing.

Proof-of-Deposit

Another method of proof operations used by many institutions is that of single pocket proof-of-deposit (POD). Under this method, all items are pre-encoded except for the dollar amount. The dollar amount is encoded in the proof operation and debit and credit items are sorted into one pocket. As each credit is entered, the amount is locked into a register. The corresponding debits are then entered and the amount of each debit is subtracted from the credit amount. No further credits can be entered until the preceding

credit is reduced to zero. This method proves each deposit as well as an overall debit and credit totals.

The POD items are then processed through multipocket reader sorters and sorted by transaction type. Computer dollar totals are accumulated for each pocket for posting to the respective general ledger accounts. Rejected items are generally posted to overnight general ledger suspense or holdover accounts and prepared for resubmission through the proof department. In institutions that charge the appropriate general ledger control account with the proof department totals for the day, totals representing rejected items are reversed the next day. These rejects are again prepared for resubmission and given to the proof department with the next day's work.

In institutions with advanced systems where the general ledger has been automated, the daily entries are accumulated in batches at the individual or central proof departments. The entries are charged to the data center through the head office clearing account, branch clearings account or a computer work-in-process account and forwarded for processing. In these institutions, the data center charges the total of captured and rejected items back to the clearing or work-in-process account. Branch and user department personnel manually prepare entries as required. In other institutions, as processing of each major application is completed, the resulting general ledger entries are generated by the computer, i.e., branch/user personnel do not have to prepare manual entries to update the general ledger. Items for the day that cannot be processed are returned to the originating branch or user department and charged to them through a control account (e.g., unposted debit/credit account).

Unposted transactions should be researched by the user department or office that submitted the items, then reversed from the control account with entries posted to the proper customer or detail account. When the general ledger is automatically posted, the branches or departments should be restricted from making manual entries directly to control accounts without passing the items through the normal process.

Optical Character Recognition

Another means of capturing data similar to MICR capture is by Optical Character Recognition (OCR). The data is either printed or typed on forms using a special type font. An OCR machine then reads the data as input. This method is now being added to some MICR reader/sorters to reduce reject rates and is widely employed in credit card operations. OCR, however, is not in common use in the financial industry.

BATCH PROOF AND BALANCING CONTROL

Upon receipt at the data center, the branch or department work is prepared for processing on high-speed MICR reader/sorter equipment. Each batch of debits and credits should contain a batch header or adding machine tape listing indicating the total dollar amount of the items included in the batch. Usually, a clerk encodes a batch number on a batch header card provided, or creates a batch header and assembles the batches into blocks of items. Each block has a header card that contains the total dollar amount of all batches in the block and a block number.

Blocks are then processed through the reader/sorter equipment and the MICR information captured by the computer. Items rejected from the initial capture run may be run through a second time. The resulting rejects should be maintained separately and sent to the reconcilement clerks with a hard copy listing of captured items. This hard copy listing contains:

- Batch number.
- Block number.
- Item capture number (each item is sequentially numbered on some systems for tracing purposes).
- Account number.
- Dollar amount of each item.
- Batch and block dollar control totals.
- Dollar amount that each individual batch and block are out of balance.

After MICR capture, the work is balanced and reconciled by the user department. A reconcilement form has the total dollar amount of debits and credits submitted for processing and tape listings of the dollar amounts in each batch. These forms and listings assist in reconciling the work submitted for processing to the captured item and the rejected item

totals.

The reconcilement clerks balance each batch of debits and credits to the batch capture reports as soon as the report is produced. As each batch is balanced, entries that were not captured on the first or second run are accumulated, and a tape listing is made of the dollar amount of each item. These rejected items are sent to the department that handles reject reentry items. The reject items are then processed with the normal work. Entries that are rejected again are returned to the reconcilement clerks for final balancing, then to the user department for research and correction.

Check Inclearings

Many financial institutions have arranged to exchange local check inclearings (checks drawn on themselves that have been deposited at other financial institutions) to be delivered directly to the data center that services the institution. The inclearings are usually received at the data center during the early morning hours of each work day and posted to depositors' accounts. Settlement between the drawee institution and the deposit financial institution may be made through the Federal Reserve Bank, local clearing houses or a correspondent financial institution.

In such cases, the financial institution upon which the checks are drawn is notified of the total dollar amount of items by advice, and the data center receives the actual items. Inclearings are processed during the day in the same manner as checks processed at night when the day's counter work is received from the financial institution. When the reconcilement clerks complete the reconcilement procedures for the financial institution's counter work, the dollar totals for the inclearings received that morning are combined with the counter work totals. The reconcilement form submitted by the user is completed to show:

- Total dollar amounts received from the financial institution.
- Total dollars received through the inclearings.
- Net captured good items and items drawn on other financial institutions that were missorted.
- Rejected items.
- Holdover items.

The beginning and ending totals of the reconcilement should balance unless any free items (enclosed not listed) were sent and not charged to the data center or items were omitted (listed not enclosed) from the shipment. In these cases, the dollar figure of transactions charged to the data center is incorrect. Therefore, appropriate adjustments should be made on the reconcilement form, and the user area or institution should be notified.

Most data centers attempt to retain the checks captured during the initial run in batch and block sequence until reconcilement clerks have balanced all the work for the day. In some data centers (usually high-volume centers), this is not considered practical and the entries are fine sorted immediately after the primary capture into the financial institution, branch and account number sequence.

Microfilming

Before transporting source documents from branches or departments for item processing, all items should be microfilmed or duplicated. Although most institutions microfilm checks that are sent to other financial institutions, they may not microfilm checks, deposits and internal entries processed to their own accounts when the items are transported to their data center or a service bureau. When shipments of the transaction documents and checks are not recorded on microfilm, the financial institution's senior management should be aware of the risk posed by loss of the shipment while in transit.

TERMINAL ENTRY

Manually entering data into computers via terminals is a common practice. Most widely used are key-to-disk or key-to-tape terminal entry systems. In these systems, data from source documents is entered on magnetic media via key-to-disk or key-to-tape equipment. Data also may be entered directly into the application files from a user department terminal. Electronic input may be received directly from teller terminals, automatic teller machines (ATMs), Point-of-Sale (POS) terminals, client-server terminals, PCs, etc. In terminal entry system, input can be displayed on a video screen as it is entered, edited manually or programmatically, and stored in memory for verification. Key-to-disk and key-to-tape systems are able to produce statistical information to monitor the

efficiency of the data entry department. All systems should be able to provide audit trails including source, operator ID, terminal ID, date, and time.

Errors can easily occur when operators convert data from source documents to a machine-readable form. Rejects can be significantly reduced if during manual entry, operators are informed of input errors which can be immediately corrected. Terminal software programs and system software can provide a high degree of error control by using the following techniques:

- Character/field count – A check of character and field count totals for comparison against totals generated as a result of the original data entry. This would indicate the loss or addition of characters or fields to magnetic data file media.

- Truncating fields – An automatic provision which provides right round off or truncation of fields which exceed maximum length.

- Checks for completeness – Programmed checks to ensure that all required entry fields are filled.

- Dollar and item count totals – A necessary tool to prove key entered batches of dollar and non-dollar transactions to preestablished control totals.

- Reasonableness checks – Programmed comparisons of data entered to predetermined absolute values or relative limits of reasonableness.

- Dual-field entry – When the same input appears twice, a check is made to ensure that both fields match.

- Verification check – Input data is echoed back to operator usually on CRT for validation.

- Sequence checks – Programmed checks of key fields in records to ensure proper sequence of data entry.

- Check digits – System performs an algorithmic operation on numeric fields, the result of which should determine the last digit used to ensure valid account numbers.

The software programs providing this type of control should be secured and written, or modified only by programmers with adequate security clearance. Additional controls used before to processing to ensure the integrity of data entered include using hash totals, block and record counts, and cross footing balancing.

Similarly, input editing, other programmed controls and control totals should be employed in on-line file maintenance and memo posting programs.

Batch control totals can be developed for terminal entries by listing and accumulating the dollar amount fields at the user level (some key-disk or tape units do this automatically). Batch totals should be developed for the dollar amounts on entries to achieve effective control. Specially prepared payment cards are used on some applications, principally installment and real estate loans. These cards are produced when the accounts are initiated. The payment coupons are pre-encoded and preprinted with the account number, the dollar amount, type of account and, in some cases, the month payment is due. The payment coupons also can be batched and totals developed for control purposes.

Data entry departments should have documentation containing illustrations of all types of input forms processed with complete step-by-step instructions entering the information on the form. The manual should serve as a training guide for new operators and for day-to-day reference. The key-to-disk and key-to-tape systems can retain and display on the video screen a format of each input form used, showing the data fields that are supplied with input.

In summary, non-MICR documents submitted for data entry that have dollar totals on the entries should be batched and totaled. Control totals for the day's work and a reconcilement form must be given to the data center. After capture, the reconcilement clerks must reconcile the output batch by batch to the item processing capture reports. All other verification of data entry source documents should be performed through a second, independent keying operation or by clerks in the user department. Whenever control totals are developed for data entry work, the work should be charged to and from the data center to ensure accountability.

OUTPUT DISTRIBUTION AND CONTROL

A financial institution's confidential information records must be protected regardless of the media

they are recorded on. All printed output and processed source documents must be safeguarded to ensure that the material is forwarded to the appropriate user departments. This section addresses the distribution of output reports in paper form. However, distribution considerations may include Remote Job Entry (RJE) transmissions; network and desktop printers; on-line terminal reports; and CD-ROMs. Whatever method is selected to distribute report information, controls should be established to ensure the proper and timely distribution of the report media.

One method of ensuring proper distribution is to establish a distribution function or department similar to that of a mailroom. Whether output reports and source documents are distributed by messengers, common carrier, or privately contracted courier service, delivery receipts for all data containers should be obtained. Courier containers with transported items should be locked; the data center and user each should have a key.

A distribution control manual should be available which contains:

- A listing by name of all reports produced for applications processed.
- Decollation and bursting instructions as required.
- The number of copies of each report produced for each branch or department.
- Each report's frequency.
- The priority for each branch, department or report in the delivery schedule.
- Special handling instructions.

Separate checklists should be developed to record all daily, weekly, monthly and quarterly reports produced for each application. Procedures should ensure that all required reports are received by the distribution department. A computer program can be written that will generate a list of the day's reports and indicate whether or not the report was produced. Alternatively, the list could reflect only the reports produced or not produced. Such a checklist should be used by both the distribution department and the user department. User areas should review output received for acceptability and consult the report checklist to determine compliance with established distribution policy. Requiring users to sign or initial receipts for computer output may further data control.

The institution's distribution department should review all reports for legible printing, proper alignment of forms and possible errors (such as lines of unsuppressed code or strings of meaningless characters). Also, control totals appearing on related reports should be cross-checked to help ensure their accuracy.

Many data center installations are using computer output microfilm (COM) to replace paper reports. A COM device takes report information from a computer and records it on microfilm. It saves considerable storage space and is far cheaper than paper output. The most common microfilm recording media is microfiche, a card containing multiple images that is displayed on a viewer.

A financial institution's confidential information records must be protected regardless of the media they are recorded on. Controls over the processing, handling and transporting of COM media must be at least as secure as those for other file media. Controls must be established over the number of copies produced and the storage or disposal of all copies. The portability of this type of media (relatively small sheets of film needing only a simple projection device to be read) underscores the importance of strict accountability and access control over this output media.

REVIEW AND RECONCILEMENT OF OUTPUT

The user or an independent control department should reconcile all entries from daily processing to the totals established when the entries were submitted and to the respective general ledger control account. Adjustments must be made for inclearings received at the data center, entries that were missing, extra entries and rejected or nonpostable entries.

In reviewing output, the user area or an independent control department should:

- Double check figures on the transaction reconcilement form originally submitted to the data center.
- Double check the figures prepared by the data

center on the transaction reconcilement form.

- Complete an additional reconcilement form for balancing the trial balance and other report totals to the general ledger control account.

When the general ledger is automated and posting entries are made by the computer, the application totals will tie into the general ledger figures without adjustment. In such cases, it is necessary to investigate the controls over rejected and holdover items and to determine the propriety and age of items in suspense accounts.

Using the demand deposit application as an example, checks captured and posted as good items normally will be reviewed when they are filed. Captured deposits may be filed with checks and returned to the customer or they may be stored by the financial institution for reference. In some institutions, larger dollar amount deposits are compared to the daily posting journal or the check file drawer and the signature card to verify the number and name on the deposit. All other entries, such as rejects, nonreads, and nonpostables, must be reviewed individually.

Inadequate reconcilement procedures by the data center's independent control section or in the user areas may impair the financial institution's ability to return forged, dishonored, or otherwise invalid items within time limits specified by the Uniform Commercial Code, clearing house associations, and various federal rules and regulations. If the return of large negotiable items is delayed, the institution risks significant monetary losses.

All rejected, nonreads, nonpostables, etc., should be segregated from captured items. Each such item should be reviewed by a clerk who either corrects the item for resubmission and posting or returns it to the user area/institution for correction and resubmission, or other disposition. All reject re-entry items should be reviewed by the user department manager. The manager ensures that entries are corrected properly and that the same items are not reappearing as unprocessable. Without such a review, a clerk could conceivably "roll" checks as unprocessable items for extended periods of time.

Exception reports always should be required output regardless of the presence of exception activity or other controls. These reports ensure that both the presence and absence of exceptions are reported. All exception reports, e.g., overdraft, large items, stop/hold, uncollected funds, kiting suspects and past due reports, must be reviewed by financial institution's officers. All reports produced as a result of nonmonetary changes should be compared with the original input, i.e., name and address, new loans, by the responsible user area. Financial institution employees originating or accepting change from a customer should be identified in writing. Also, only under unusual circumstances should master file changes be done without written documentation initiated by the customer.

The responsibility for balancing transaction and trial balance reports to the general ledger often is delegated to a clerk in the user department or to a centralized control division. Periodic unannounced reconcilements should be performed by the institution's auditor or a designated control officer to ensure compliance with established operating procedures. An unannounced reconcilement should include a review of the department settlement sheet, unposted items and exception reports. All large or unusual items should be traced to their final disposition. Records of the reconcilement must be maintained by the auditor or designated control officer, noting the dates of the reconcilement and a listing of all exceptions. Department records should be initiated by the person conducting the check.

This section is intended to review the physical and functional aspects of the data centers operations for the presence of adequate procedures and controls. The work program should be used with the Operations Section narrative, which provides overall guidance. Also obtain access to reference manuals as an aid in performing the examination. Manuals with titles such as "Planning and Installation Guide," "Operational Principles," "Administrative Guide," and "Auditors Guide" can be particularly helpful. This section is used to review compliance with established policy and assess the soundness of physical and internal controls. The examination procedures in this workprogram should be coordinated with those in the Corporate Contingency Planning (Chapter 10) and the Security Physical and Data (Chapter 14) workprograms. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*. This document will become part of the workpapers.

Tier I

GENERAL

1. Identify the hardware and the operating system(s) in use.

MANAGEMENT REPORTING AND PLANNING

2. Review and evaluate the method(s) and frequency for monitoring system performance. This could entail:

   a. Monitoring continuously (if this is a large facility),

   b. Measuring whenever there is a change in the system configuration, or

   c. Measuring periodically to account for changes in loading (due for instance to increasing account volume).

3. In connection with systems performance monitoring and capacity planning, determine whether hardware/software constraints (choke points) have been identified, and evaluate their effect on operations.

4. Determine whether a job-accounting system is utilized.

PHYSICAL ENVIRONMENT

5. Does the computer room have an adequate and safe fire-suppression system with associated detectors

(heat, smoke, water), and are other necessary environmental controls in use?

6. Identify any obvious safety hazards to people or equipment.

7. Review the adequacy of the UPS system.

8. Determine if sensitive forms, negotiable items (checks, stock certificates, etc.), and signature plates are adequately controlled.

EQUIPMENT MAINTENANCE

9. Review log for equipment malfunctions.

10. Determine the existence of a program of regular preventive maintenance.

11. If any equipment is maintained by an outside vendor, review the maintenance agreement for reasonableness.

12. Review the performance of the maintenance vendors. If not, satisfactory, identify the corrective action.

OPERATIONAL PROCEDURES

13. Review the experience levels and training provided to the computer operations staff.

14. Review the operations procedures manual used by computer operators. Determine whether, according to those procedures and in practice, operator duties are properly segregated.

15. Review the console log. Determine whether it is reviewed by supervisory personnel and retained for a reasonable of time in safe storage to provide an audit trail.

16. Review the job scheduling function and assess its adequacy.

17. Review the problem reporting/resolution tracking system and determine whether:

    a. Problems are appropriately logged and prioritized

    b. Corrective measures are implemented in a timely manner.

c. Management reporting procedures are adequate.

18. Determine whether computer output is protected from unauthorized access, (i.e,. by placement in locked bins assigned to specific individuals or departments).

EMERGENCY PROCEDURES

19. Review and assess the adequacy of the organization's emergency procedures.

BACKUP

20. Review procedures for the creation and rotation of backup media (disks or tapes). Coordinate this review with the procedures performed in the Corporate Contingency Planning workprogram in Chapter 10. Determine whether backup procedures provide for the ability to adequately recover:

    a. Operating systems.

    b. Application programs

    c. Master files

    d. Transaction files

    e. System utilities.

    f. Any other programs that are necessary to restore operations at the recovery site.

21. Determine if backup media (disks or tapes) is rotated off-premises in a timely manner.

22. Determine if the off-site storage facility is:

    a. Sufficiently remote from the processing facility.

    b. Adequately controlled for access and environment.

    c. Accessible within a reasonable time frame if backups are needed.

23. Determine whether PC-and LAN-based data and systems backed up as is the mainframe and the backed copies are kept remote from the hardware.

TAPE LIBRARY

24. Determine whether a tape management system is in place.

25. Identify what prevents unauthorized removal, introduction, or substitution of tapes.

26. Identify what prevents the mounting and use of the wrong tape.

27. Identify what prevents the inadvertent use of an active tape as a scratch tape.

28. If a tape management system is in use, verify that only appropriate personnel are able to override its controls, for instance by use of an operating system feature that bypasses processing of the tape's magnetic labels.

ITEM PROCESSING AND DATA ENTRY

29. Determine the adequacy of controls for input and output processing and record retention.

CONCLUSIONS

30. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

31. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

c. Management's proposed actions for correcting deficiencies.

32. Assign rating (see Chapter 5 for additional information).

33. Prepare an index of workpapers for this section of the workprogram.

34. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions, and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

35. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

MANAGEMENT REPORTING AND PLANNING

1. Determine whether performance is reported to management regularly. Obtain a copy of the most recent report(s). They should include:

   a. Response times.

   b. Throughput.

   c. Proportion of downtime.

   d. Frequency and maximum duration of outages.

   e. Proportion, types and causes of job failure.

   f. Computer system peak and average utilization, and trends.

EQUIPMENT MAINTENANCE

2. Review the equipment malfunctions log for patterns of recurring malfunction or repair that have resulted in frequent disruption of operations and/or excessive cost.

3. Review whether management is aware of each problem and has made a decision about whether or how to correct the situation.

OPERATIONAL PROCEDURES

4. Review the operators' duties and determine whether they are prevented from:

   a. Originating entries for processing.

   b. Correcting data exceptions, unposted or rejected items.

   c. Preparing any general ledger and/of subsidiary ledger entries.

   d. Performing any balancing functions (reconcilements) other than run to run control.

   e. Running test programs against live or backup files.

f. Executing programs from the test library during production runs.

g. Controlling report generation and distribution.

5. At entities where one person performs more than one of the above functions, are results checked by an independent person.

6. If operators can override system security are such activities logged and reviewed.

7. Are lengthy and resource-intensive jobs scheduled for execution during non-peak times.

8. Do exceptions to the job schedule require authorization. Are exceptions logged and reviewed.

9. Determine how the source and authorization of production jobs is verified.

10. Are disk packs scanned periodically for obsolete and/or inactive datasets and are those datasets deleted or migrated to tape.

EMERGENCY PROCEDURES

11. Determine if the posted emergency procedures address:

    a. Instructions for shutting off utilities.

    b. Instructions for powering down equipment.

    c. Instructions for activating/deactivating fire suppression equipment.

    d. Personnel evacuation.

    e. Securing valuable assets.

12. Determine if emergency procedures are conspicuously posted throughout the organization.

13. Access whether employees are familiar with their duties and responsibilities in an emergency situation and whether an adequate employee training program been implemented.

14. Determine if the organization periodically conducts drills to test emergency procedures. And access whether drills are monitored to provide feedback on the effectiveness of established emergency procedures and employee training.

TAPE LIBRARY

15. After the expiration date of a tape data set, determine if the data still be read by anyone who knows the identity of the volume.

16. Determine whether:

    a. The tape library is environmentally controlled.

    b. Tapes including backups are tested periodically for defects.

17. Determine if the data center can produce a report showing all tapes on hand and:

    a. How frequently is the inventory updated.

    b. Whether off-site tapes accounted for.

    c. If the inventory includes:

    - Volume name/number.
    - Location.
    - Names of all files on the volume.
    - Creation and expiration dates of the contents.

ITEM PROCESSING AND DATA ENTRY

18. Determine if source document images are recorded for recovery in case the originals are lost in transit.

19. Note whether batch dollar totals are reconciled after processing.

20. Determine if each batch is associated with a responsible individual.

21. Note whether batches are of a reasonable size so that out-of-balance conditions can be reconciled easily.

	Comments
22. Determine if there is automated checking of data input (e.g. field counts, entry length measurements, reasonable-value tests, etc.).	
23. Determine whether reject items are properly segregated from other work.	
24. Note whether exception items are adequately controlled and tracked.	
25. Assess whether items are allowed to remain in suspense status for extended lengths of time.	
26. Proceed to procedure 30, Tier I.	

Examiner | Date

_____|_____

Reviewer's Initials

SECURITY - PHYSICAL AND DATA CHAPTER 14

(FILE NAME ON DISK # 1 = S2C14.WPD)

One of the most important assets of an organization is information. As such, protecting or securing information and facilities that process and maintain information is vital to operations. The impact of security deficiencies are lost business, damaged reputations, fiduciary losses, lost assets, and possibly lost trade secrets. Security controls are needed to safeguard information from unauthorized or accidental modification, destruction, and disclosure, and to ensure timeliness, availability and usability of data. Possible threats to operations include ignorance and carelessness, fire and water damage, disgruntled or unethical employees, outsiders or hackers, and viruses.

The organization needs a comprehensive written security plan to minimize exposure to all threats and risks. This program should emphasize the need for asset protection, security, and controls. The degree of control should be based on an assessment of risk in relation to the value of the asset. It also should reflect proper concerns for the sensitivity of information. Three major areas that must be reviewed to ensure that IS operations and information are not vulnerable to undue risks and exposures are: physical security; data security; and backup and contingency planning. This chapter focuses on the first two risk areas. Corporate contingency planning is discussed in Chapter 10.

SECURITY ADMINISTRATION AND ACCOUNTABILITY

Management must regulate and monitor the computer environment by establishing security standards, policies, procedures, and controls that are incorporated into the organization's normal business practices. Maintaining a secure environment requires ongoing vigilance. After establishing a security plan, security procedures should be developed to ensure the plan's provisions are followed, and threats to the system are quickly detected. Responsibility for security should reside with the security administrator and/or information security personnel. The security administrator or information security personnel must be familiar with the organization's overall security policies and should have the authority to recommend and implement controls in strategic areas. They also should, if acting as LAN administrator, be thoroughly familiar with the LAN's administration. Personnel departments should be responsible for tracking all terminations and providing notification to the appropriate security personnel. Depending on the size of the organization, security measures can range from simple file scanning to full-scale surveillance of equipment and data files. Such measures also may include issuing user identification codes, maintaining and establishing user security levels, and controlling access to sensitive data and program files. In general, security administration responsibilities should include:

- Performing risk analysis.
- Establishing, enforcing and monitoring the security program for all platforms (mainframe, minicomputer, LANs, and PCs).
- Acting as a liaison between users and management.
- Reviewing user access codes periodically for appropriate access levels.

Personnel assigned security administration duties also should not be involved with input authorization and preparation, computer operations, programming, or output reconciliation duties. Proper segregation of security functions is not always possible in institutions with limited staff. In those cases where segregation of duties is impractical, management should ensure an appropriate independent review of security administration activities is conducted by a knowledgeable third party. In smaller institutions this independent review may be conducted by a non-involved manager or senior officer.

Security administration for a PC may be different than that on a mainframe, minicomputer, or LAN. Mainframe and LAN administration is centralized

through the use of security software. PC software is implemented and administered on each individual unit. Because computers are widely distributed throughout the financial institution, the administrator may need to delegate immediate supervision to designated persons within user areas or assign a departmental security contact who is responsible for overseeing and coordinating the area's security requirements and controls. These individuals in turn would report security violations to the security administrator.

SECURITY PLAN

An overall security plan includes: physical protection of the data facility and IS equipment throughout the organization and data security. The plan should be developed with the approval and involvement of top management and the board of directors and cover all functions performed in the IS operation and all areas touched by automation. Senior management's commitment to security should be emphasized and provisions for communicating security objectives to all employees should be clearly specified.

Security of the IS operation must be integrated with the security plan of the entire organization. Capable senior officials should be charged with its development, implementation, and administration. Generally, their responsibilities fall into two areas: the design of security techniques, and procedures for day-to-day security operations. Extensive security measures will be ineffective if not properly implemented. Therefore, active employee participation and enforcement at all levels is vital. A well-developed security training program that includes regular a review of security procedures will reduce the vulnerability of the organization. Properly trained IS auditors can independently assess the extent to which a formal security plan is being followed and may play a key role in assuring its adequacy.

The first element of the plan is concerned with physical protection of the data processing facility and all computer equipment. It should include measures to minimize exposure or the probability of threat to all computer hardware and software throughout the organization. Computer resources within the institution should be ranked in order of importance and protected with a commensurate level of security. Identification of the protection provided, the significance of specific threats, and individuals responsible for execution of the program should be specified in the plan. Using technical and administrative precautions, together with operational and procedural controls, will help reduce the probability of accidents. A description of electronic or mechanical devices selected to prevent and detect physical threats also should be included. Management may want to restrict access to this sensitive information so that protection measures are not compromised. The security program also must consider proper insurance provisions as detailed in Chapter 9.

The second element of the security plan should include proper preventative and detective measures to reduce the risk of interruption of business due to unauthorized access and manipulation of data and programs, and inaccurate or incomplete processing. The accuracy and integrity of data is depends on proper control procedures for processing in both the user and data processing areas of the institution.

USER EDUCATION

Users have varying levels of expertise and familiarity with computers. A user education program should be implemented to promote awareness regarding the use and care of computers and their obligation to challenge any person or procedure that may violate security systems. Users should have operation and procedural manuals available for reference. Training sessions should be held during equipment installation. Additionally, training should be included as part of new employees' orientation whose duties involve using computers. Suggested topics for training sessions include:

- Corporate policy regarding the use of computers.
- Data security policies and procedures and their implementation.
- User involvement and responsibility toward promoting data security.
- Disciplinary action taken when data security policies are violated.

PHYSICAL, BUILDING, CABINET, AND VAULT SECURITY

An uninterrupted IS operation depends upon provisions to prevent, detect, minimize, and recover losses from damage or unauthorized use of equipment, software, or data. Protective measures against intentional and accidental threats should be included in these physical security measures.

A physical security plan should be designed to obtain maximum protection at a reasonable cost. Although it may not be practical to completely safeguard a computer installation, thorough evaluation of alternatives is important. This evaluation should include a risk assessment that consists of determining what needs to be secured (e.g., information, equipment, personnel, network services such as E-mail, applications, software, etc.), sources of risks (e.g., environmental occurrences, viruses, hackers, and unethical employees), probability of occurrence, costs and remedies available to minimize exposure.

Physical security must be coordinated with the entire data processing operation and not regarded as an independent function. Controls and procedures, such as backup, housekeeping, auditing, and documentation, supplement the protection provided by physical security measures. It may be difficult to quantify or assess the success of physical security efforts. However, with proper management support and employee training, the overall effectiveness of all IS operations is enhanced through such safeguards.

Building Security

When selecting a site for a computer facility, management's major objective is to limit the risk of environmental exposure from internal and external sources. The selection process should include a review of the surrounding area to determine if it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Outside intruders can be deterred through the use of guards, fences, barriers, surveillance equipment, or other similar devices. Since access to the data center should be limited, doors and windows must be secured.

Some intruder detection devices available include:

- Switches that activate an alarm when an electrical circuit is broken.
- Light and laser beams, ultraviolet beams and sound or vibration detectors that are invisible to the intruder.
- Ultrasonic and radar devices that detect movement in a room.
- Closed-circuit television.

The detection devices should provide continuous coverage. Security guards should be properly instructed about their duties. The data center employees who access secured areas should have proper identification, such as badges. All visitors should sign-in and wear proper IDs so that they can be identified easily. Detection devices, where applicable, should be utilized to prevent theft and safeguard the equipment. Security guards should be educated as to who is permitted to remove assets from the premises and record the identity of anyone removing them. Consideration should be given to implementing a specific and formal authorization process for the removal of PCs from the premises.

Actual building security precautions will vary depending on size and location of the data center and/or institution. If the center is located in a separate building, extensive security precautions may be appropriate for the entrances and perimeter. If the institution is housed in an office building, security precautions should focus on entry from other areas of the building. Many computer centers use magnetic encoded key cards to unlock doors. In many cases these systems are managed by a PC and will maintain a daily access activity log the time of day access was provided. Key cards may be selectively encoded to allow a proof operator, for instance, to gain entry to the computer center but not to the computer room. The cards also may be encoded for specific time-of-day entry to further their control. In addition, extra precautions should be taken to physically secure cabling when floor space of a building is utilized by the organization versus a separate building. It would be much easier to tap the wiring in a building that is shared by other tenants rather than a building in which the institution is the sole occupant.

Cabinet and Vault Security

Protective containers are designed to meet either fire-resistant or burglar-resistant standards. Labels describing expected tolerance levels are usually attached to safes and vault doors.

PHYSICAL SECURITY FOR PCS AND DISTRIBUTED IS ENVIRONMENTS

A computer located in a user department is often less secure than one located in a computer room. Minicomputers or other distributed data processing environments (e.g., Local Area Networks or LANs) that offer a full range of applications for small financial institutions as well as larger organizations are commonly housed throughout the organization, without special environmental controls or raised flooring. In such situations, physical security precautions are often less sophisticated than those found in large data centers, and overall building security becomes more important. All computers, however, should be physically separate from other financial institution operations and internal control procedures should be established regardless of the size of the computer. The level of security surrounding any computer should depend on the significance of the applications processed and risks to the organization, the cost of equipment, and the availability of backup equipment.

Because of their portability, PCs often are prime targets for theft and misuse. The location of PCs determines the extent of physical security required. PCs located in unrestricted facilities should, at a minimum, be protected by a physical barrier – such as a counter or divider – preventing easy access by customers. Employees also should have restricted access to PCs and data. The sensitivity of the data processed or accessed by the computer usually dictates the level of control required. The effectiveness of security measures depends on employee awareness and enforcement of these controls.

An advantage of PCs is that they can operate in an office environment. This provides flexible and informal processing operations. However, as with larger systems, PCs are sensitive to environmental factors such as smoke, dust, heat, humidity, food particles, and liquids. Because they are not usually located within a protected data processing center, housekeeping practices should be adapted to provide protection from ordinary contaminants.

Other environmental problems to guard against include electrical power surges and static electricity. The electrical power supply in an office environment is sufficient for a PC's requirements. However, periodic fluctuations in power (surges) can cause equipment damage or loss of data. PCs in carpeted areas are susceptible to static electrical discharges that can cause damage to PC components or memory.

Physical security for distributed data processing, particularly LANs, which are usually PC-based, is slightly different than for mainframe or minicomputer platforms. With a network there is often no centralized computer room. In addition, a network often extends beyond the local premises. There are certain components which need physical security. These include the hardware devices and the software and data that may be stored on the file servers, PCs, or removable media (tapes and disks). As with the traditional mainframe or minicomputer environment, physical network security should prevent unauthorized personnel from accessing LAN devices or the transmission of data.

Physical protection for networks as well as PCs includes: power protection, physical locks, security guards, magnetic badge readers, secure dial-up modems, diskless workstations, data encryption, and backups. Physical access to the network servers (files, applications, communications, etc.) should be off limits to anyone but the LAN administrator. Network workstations or PCs should be password protected and monitored for all workstation activity. Network wiring requires some form of protection since it does not have to be physically penetrated for the data it carries to be revealed. Network security also can be compromised by capturing radio frequency emissions.

PERSONNEL, DATA FILE MEDIA, AND COMPUTER OPERATIONS SECURITY

Personnel security is vital to the overall security plan. The quality of the data processing function and organization is directly related to the quality of its personnel. Most computer systems are vulnerable to staff tampering. Implementing security controls over personnel and assigning responsibility for monitoring and enforcing these procedures play a major role in

establishing a sound operation. In addition, adequate security over computer operations can yield secondary benefits, such as error-rate reductions, improved quality, better scheduling, and more timely results.

Written operating procedures should be current and sufficiently detailed to guide the organization and operation of the computer center. Access to the computer room must be restricted to authorized personnel. The best environment is created when only the computer operations personnel (operators and supervisors) are allowed in the computer room.

Computer operators should be denied access to program flowcharts, source decks, program listings, etc., since they are not required to perform programming duties. These items should be secured and maintained outside the computer room to prevent unauthorized changes to programs by computer operators.

Programmers, input/output control clerks, systems analysts, consultant engineers, etc., should be restricted from entering the computer room. All work should be delivered and picked up through dispatch windows or a scheduling department. If an authorized visitor requires admittance to the computer room, regular check-in and check-out control procedures should be followed. The physical layout of some computer facilities may not permit complete restriction, particularly if the tape/disk library is located within the confines of the computer room. The computer room should be locked at all times and exits should be readily accessible from the inside.

The tape/disk file library should be protected from physical disaster in the same manner as the computer room. In addition, the library should be controlled throughout all operating shifts to prevent unauthorized access to data file media. During shifts in which a librarian is not present, alternate procedures may be implemented. All media within the library, such as magnetic tapes, disk packs and cards should be stored in a closed, dust-free, fire-resistant area. Removal of these files from the library should be permitted only when needed for processing. In addition, all critical data and software on the various media should be backed up and stored off-site. This provides an easy recovery should a crisis occurs.

Control of sensitive forms is another important security concern. Printed forms of a negotiable nature (checks, stock certificates, etc.) and signature plates are vulnerable to misapplication and must be secured. Appropriate controls include dual control locks for forms within a secure location and inventory records that specify date, time of access, and personnel accessing the secure location. The supply of forms should be issued according to scheduled production runs. Periodic inventories should be completed for all forms. Any checks that are voided during processing should be distributed to appropriate users for accountability.

The physical security plan also should address the personnel and data media protection for the equipment, data, and software necessary to operate the PC and local area networks. All LAN-based servers should be located in a secured room. Access to the servers should be limited to LAN administrators and other computer operators if necessary. It is unlikely that the physical access to standalone PCs can be secured. If the PC cannot be housed in a secured area, such as behind a locked door or in a locked drawer, a key entry system or software security must be in place to prevent unauthorized users from accessing the unit.

Storage devices for PCs and LANs (such as hard disks, diskettes, and tape media) can be damaged by excessive heat, smoke, dust, liquids, and other contaminants. Diskettes, the most common medium of storage, are more sensitive and require more care than hard disks and tapes. It is important that all personnel learn to handle diskettes properly. All data media should be externally labeled to identify contents and avoid mishandling. Diskettes and tapes should be stored in a physically secure location when not in use. Backup and off-site storage is necessary for key data to ensure proper recovery.

HARDWARE AND SOFTWARE INVENTORY

The inventory system should record all hardware, including terminals, servers, PC equipment and peripherals. This includes their purchase, distribution and disposal. A hardware inventory should include:

- Manufacturer's name and model number.
- Identifying serial number.

- Cost.
- Date of purchase.
- Current location.
- Name of user or user group responsible for use.

A hardware inventory system should facilitate resource sharing, software distribution and maintenance, and repair or replacement of equipment. To ensure proper record keeping and compatibility with other hardware and software in use, ordering and distribution of hardware should be centralized under the authority of the information systems department. All security administrators should receive a copy of the most recent inventory listing.

Software Inventory

All software, whether purchased or developed in house, should be accounted for through an inventory system. Additionally, vendor contracts for purchased software should be centrally maintained. Inventory maintenance is important because it:

- Facilitates locating software for replacements or upgrades.
- Can be used to identify what software is executed at a particular PC and the person(s) accountable.
- Reduces risks of violating software licensing agreements (for purchased software only).
- Provides internal controls for institutional assets.

The inventory listing should include the following information:

For purchased software:

- Date of purchase.
- Product and manufacturers' names.
- Identify whether purchased outright or under a licensing agreement.
- Cost.
- Version number.
- Serial number.
- User area where installed.
- Number of copies installed for use on the server.

For in-house developed software:

- Program name.
- Program developer.
- Initial date of creation.
- Date last updated.
- User area where installed.

The individual responsible for all software acquisitions and maintenance should have an up-to-date copy of the inventory listing. This individual also should be aware of contract terms, such as copyright restrictions and maintenance responsibilities.

Copyright Protections

Purchased software is usually licensed for use rather than purchased outright. Such proprietary software is protected by copyright. The license specifies how many copies the financial institution is entitled to and may identify which machine(s) and how many users may use the software. Violations of the licensing agreement expose the institution to possible costly litigation. In addition, illegally installed software may ultimately lead to operational inefficiencies. For example, effective maintenance would be difficult to implement since unauthorized copies of software would not be recorded in an inventory system. This may result in unauthorized users utilizing obsolete versions.

Caution should be taken when purchasing network software. Many software programs are not licensed for shared use on a network. Individual copies must be purchased for each network user. There are software packages that can be acquired for a network that allow only a predetermined number of persons to utilize the programs concurrently rather than acquiring a licensed copy for each individual user on the network. For example, instead of purchasing a licensing agreement for 100 specific users who are defined to the network, an organization may acquire a 50 concurrent usage site license since no more than 50 individuals will access that software on the network at any given time.

Adhering to copyright laws and vendor terms and conditions will protect all parties. Measures which financial institutions may employ to protect against

copyright violations include:

- Obtaining a site license that authorizes use of the software at all PC locations within the organization.
- Assuring that employees are were informed about the rules governing site licenses.

While these measures may help prevent copyright violations, the best control mechanism is having a strict corporate policy that is communicated and enforced by management and auditors. Management must have an uncompromising attitude regarding copyright violations. The security administrator should be responsible for enforcing and monitoring the policy. Users should understand that unauthorized copying and/or usage of software is both legally and ethically wrong and that this practice is unacceptable under corporate standards.

DATA SECURITY

Just as hardware has to be protected, access to software and data also has to be restricted. Software and data are valuable assets and considerable damage including financial loss could be incurred if they are lost, stolen, or compromised. Implementing and enforcing data security controls will protect the data and software resources or any information that is transmitted and stored against accidental or intentional disclosure to unauthorized persons or for unauthorized modification or destruction. The seven essentials of data security are:

- Data should be protected from fire, theft and other physical hazards.
- Data should be reconstructible to recover from destruction or loss (intentional or accidental).
- Data should be auditable for prompt detection of loss and accidental and intentional manipulation.
- Systems should be tamper proof to prohibit programmers and systems analysts from bypassing controls.
- Users must be identified before being granted access.
- Systems must be able to check that user actions are authorized.
- User actions should be monitored so that suspicious or unauthorized behavior can be investigated.

Deliberate or accidental security exposures present in all data processing environments may be heightened by certain features of automated systems. Examples of deliberate threats include:

- A trapdoor or window built into the system by a programmer.
- Dumping portions of memory to obtain sensitive information, codes, passwords, etc.
- Misuse of another person's authorized access code, password, etc.
- Obtaining access codes or other restricted data by obtaining copies of hard-copy output from trash cans, etc.
- Obtaining access codes or other restricted data by wiretapping.

Examples of accidental threats include:

- Faults in the data communication system leading to erroneous data in the data base.
- Hardware or software failures leading to a breakdown of a built-in security feature. For example, secret data – such as passwords – may be printed as part of a core dump during an abnormal termination or a recovery.

The accuracy and integrity of data as well as continued operations depend on establishing proper control procedures and guidelines for processing in user and data processing areas within the financial institution. To ensure that data is secure and operations are uninterrupted the following key elements of data security for all platforms (mainframe, minicomputer, LANs, and PCs) should be reviewed:

- Logical access security.
- Data integrity.
- Telecommunications security.

- Output distribution controls.
- Virus protection strategy.
- User education.
- Accountability.

LOGICAL ACCESS SECURITY AND CONTROLS

Logical access security prevents unauthorized users from connecting or gaining access to application and system resources before and after achieving physical connection to PCs, local area networks, minicomputer or mainframe systems. Logical access security includes logical access controls (user IDs and passwords) and programming security (systems software access).

Logical Access Controls

Logical access security objectives should include identification and authorization of users. The degree of control present within each computer system depends on how it is used. For example, PCs can be used as standalone systems or as access links to mainframes, minicomputers, or LANs. In addition, differentiation must be made between computers that can access classified information and those which only utilize nonclassified information.

Exposures within each type of usage should be determined through risk analysis conducted under the supervision of the security administrator. The rules that determine access to specific systems and information should be based on such risk analysis. Before users receive their log-on ID and password, the level of security access or rules must be defined by departmental management and forwarded to the security administrator for implementation. Levels of access or rules should be predetermined to ensure consistency between user types.

Computer capability may be limited by function. Depending on the function and the sensitivity of the application or data, protection may be implemented at the system data base, file, record, or field level. Various authorized actions include read, write, execute, and allocate. Thus, user access can be limited to those functions necessary to perform a specific job.

A user ID grants initial access, and a password authenticates the user's authorization to access the system. User IDs must be specific to one user since it will determine what a user can access and serve as an audit trail for transactions done by that user. The password must be held in strict confidence. Passwords should be changed periodically or whenever compromised. They may be of fixed or variable lengths. Passwords should be difficult to guess and must be adequately protected. Methods of protection include:

- Maintaining passwords in protected storage.
- Storing passwords in encrypted format.
- Print suppression, scrambling, or overprinting passwords when entered at the terminal.
- Printing decoys to camouflage the true password.
- Limiting the number of attempts for accessing the system, for example, after three failures, access is denied.

The security administrator is responsible for maintaining user IDs and passwords. Personnel departments should track all terminations accurately and notify the security administrator of such actions. Passwords and user IDs also should be revoked when users will be absent for extended periods. It is recommended that an individual other than the security administrator regularly review system logs and exception reports for access violations. This provides the necessary checks and balances for managing systems security. Logs serve as an effective control in any on-line system. Information contained in the logs should include:

- Unauthorized attempts to gain access to the system. Such attempts should be logged automatically by the system and a documented review of the exception report maintained by management. The system may be programmed to disconnect the offending terminal or PC from the network and to alert the responsible officer by displaying a message on the computer console or on a terminal display monitored by a security group.
- Attempts to gain information above the user's level of accessibility. These attempts also should

be logged automatically by the system. If a user continually attempts to access unauthorized information, the system should notify the responsible officer, who should investigate the reason.

- A detailed transaction file for each application. At a minimum, this file should contain information about the transaction and identification of the terminal and operator that initiated the transaction. A separate transaction file should be maintained for each accessible master file. As transactions are received from a terminal station, the date, time and sequence number are added to the file by the system. The expanded transactions are then copied onto a disk or tape. In some systems, the program acknowledges each transaction as it is received. If the system fails, the terminal operator should know the status of the current transaction at the time of failure. Reconstruction after a system failure requires a strict control procedure to limit errors. The transaction log may be used, if necessary, to reconstruct the master file by posting the entries in the transaction log to the backup master file. Thus, providing a detailed transaction file not only aids security, but also can be used to recovery in the event of an outage.

- Changes to operating system parameters, security tables, and network parameters.

Third-party security software packages for all platforms (mainframes, minicomputers, PCs, and LANs) can be utilized to prevent users from unauthorized access to the computer system itself as well as applications and data. While major strides have been made over the past few years, the LAN environment still lacks the mature industry standard security packages currently found on the mainframe.

Built in security controls also are contained in certain database management systems such as Oracle, SQL Server, and DB2. Finally, security restrictions may be programmed into an application to prevent users from unauthorized access to highly confidential information.

In addition to user IDs and passwords, logical access protection may be as simple as removing storage media (e.g., diskettes, tapes, removable hard drives, etc.) and keeping it in a secure location. Other controls include automatic log-off, time of day controls, keyboard locks, and data/file encryption.

Various types of automatic log-off mechanisms exist on mainframes, minicomputers, and PCs. In some mainframe environments the security software will automatically log an individual out of the system if no processing or keyboard action has occurred over a brief period of time (e.g., 10 minutes). With PC-based security, the software does not typically log the user off after a designated timeframe, but suspends operations. The screen or monitor will blacken or shut-off, but the user stays at the same location within the application or system. The individual only needs to type in password to resume functionality at the point of suspension.

Terminals and/or PCs used as standalones, terminal emulators, or networking devices utilize the security software on the desired platform for further controls after initial access has been granted. Once the user logs onto the system, different methods are utilized to provide control such as user profile and authorization tables. User profiles are unique to each user and extend to programs, data files, terminals or PCs, time periods of access, executable transactions and commands. Authorization tables involve classifying users into various groups with associated access levels. Software may be available, however, that enables users to circumvent system security controls. For that matter, any person knowledgeable in programming also may be able to circumvent these controls. As a precaution, files containing user IDs, passwords, and log-on sequences should be assigned the highest level of security, permitting only limited access.

While user IDs and passwords protect against unauthorized access, they do not protect against unauthorized disclosures. Computers that are part of a network need further protection because they transmit data to other terminals or PCs (standalone and networked) as well as to mainframe or minicomputers. During transmission, all nodes can read traffic on the network, thus potentially compromising data. Telecommunications security, such as data encryption, is required to assure data integrity, confidentiality, and system availability.

While encryption is required to ensure the privacy of data during transmission, it also can be used to

protect data files when other security mechanisms are unavailable, such as passwords or physical access protection. In addition, if the files are highly confidential, encryption may be used with these controls. A unique cryptographic key is used for each data file. The key used to encrypt the data is provided by the system or user. The encrypted data is enciphered before it is stored so that it becomes unusable to anyone except the person who holds the encryption key. In communication encryption, a transmitted file is decrypted at its destination, that is data is not encrypted when stored. In contrast, a data file remains encrypted until it's used again by the individual who has the key. Once a file is encrypted, the encryption key must be safeguarded against unauthorized access or loss.

PROGRAM SECURITY

Strict security should be maintained over access to and use of computer programs. Procedures should be in effect to restrict unauthorized access to:

- Application programs.
- Operating systems programs.
- Data files.
- Documentation.
- Computer equipment.

In addition, periodic supervisory review of activity logs, time records, reports, and console sheets should be required. Software programs may be used to flag exceptions. Many systems offer additional techniques to ensure program security. These advanced systems have the capability to protect libraries, produce system activity logs, and restrict operator access to unauthorized functions.

Systems utility programs are valuable tools when used during program debugging, file maintenance, cataloging, or even daily operations of the overall computer environment. However, certain programs can be used to alter storage, data files, and object code; enter the supervisor state; and catalog, purge and rename programs. System utilities also have capabilities to alter or delete programs or data. Most computer manufacturers supply these programs as part of the operating system. Commonly encountered programs include:

- IBM systems – DITTO, DEBE, IMASZAP (Superzap), IEBGENER, IEBRENAM, MSHP, IEBUPDAT, DFU, PDM, RLU, SDA, SEU, Windowtool/400, WFU, POP, RPGC, and Query/400.

- Unisys systems – Cande, Patch, Dumpall, and file copy.

- NCR systems – TRXFIX, FIX, $EDIT, and $CLEDIT.

Programs like these should be controlled to prevent unauthorized use.

Unauthorized use of system utility programs can be controlled in several ways. These controls, however, will not be effective if they unnecessarily impede operations. System utilities can be controlled by:

- Installing a password system on all program libraries/directories, including the system utility library/directory. If password protection is used, measures must be taken to control access to the passwords. Passwords should be changed periodically.

- Using automated library systems. Several automated library systems that provide program security are available from equipment manufacturers and software vendors. Such programs restrict access to the program library/directory. They can produce daily reports identifying each program that was accessed and any program changes that were made.

Even the most sophisticated security system will fail if management does not establish, implement and maintain adequate internal and operating controls. Standards and procedures for all aspects of program development, processing, and maintenance are necessary. These must identify control responsibilities and processes for documentation, review and approval of various programming activities. Supervision of these functions is imperative for establishing and maintaining program integrity. See Chapter 12 for additional information on program security.

DATA INTEGRITY

Financial institutions cannot exist without reliable data. Audit procedures must be established to ensure the accuracy and integrity of data. In addition to strong physical and logical access security, input and processing controls which consists of value, range, consistency, and reasonableness checks will improve data quality as well as processing efficiency. Program and system software control mechanisms are needed to protect the integrity of the applications, ensure valid data is entered into the system, and notify the user and appropriate personnel when erroneous data has been submitted into the system. Finally, to ensure data integrity on all systems, duties should be segregated. For more information on this topic, see the 1996 *Handbook* section titled "MIS Review" (Chapter 11).

Input and Processing Controls

Manually entering data into computers via terminals or PCs is a common practice. Most widely used are key-to-disk or key-to-tape entry systems. Data edit procedures can significantly reduce manual entry errors during input. In addition, edits can be built into programs and applications to ensure that data are being processed are valid. System software can provide a high degree of input and processing error controls.

A control mechanism to prevent unauthorized data alterations is to prohibit programmers and end-users from utilizing live data files for testing, training, and demonstrations. Program testing data or duplicate copies of actual data should be used for that purpose. In some organizations, it is common to find a centralized group responsible for providing such data and specifying test cases to run. In addition, a risk to the confidentiality and accuracy of customer data exists if data center computer devices can be used to make entries to live files or to retrieve sensitive information not required by IS operations personnel in their performance of assigned duties. Strict access and authorization controls should exist for such computers.

The proliferation of PCs and distributed processing (e.g., LANs) has resulted in data being stored and processed on multiple platforms. This causes a number of potential problems, such as the duplication of data and varying complex security access systems. In a distributed environment, data integrity is a greater risk and concern than with centralized mainframe systems. There are more opportunities to transform the data as it moves through the various systems. The automation technology is such that data from different areas of an institution is being funneled from several different, if not independent, systems which may be accurate. As an example, a report provided to the board of directors can be consolidated from 20 separate reports. Some of the data is generated by individual PCs; some connected to LANs, and others connected to the mainframe.

Another data integrity concern for network systems (e.g., mainframe, LANs, etc.) is where multiple users have access to shared data files and two or more users want to access and update the same files or records simultaneously. Software locking mechanisms can be utilized to prevent concurrent access. Several locking options include manual file locking and automatic record/file locking. Manual file locking allows the user to request that a lock be placed on the data that is to be used before to accessing the file or record. Automatic record/file mechanisms programmatically prohibits others from using data once the file/record has been accessed.

As data is transferred either manually or in an automated format between environments, the exposure to inaccuracies and/or loss of information is enhanced. Security mechanisms, such as logical access controls, automatic and/or manual cross verification of data, and programmatic and system software error controls will minimize the potential of data integrity risks.

Due to technologies that continuously change, increased end-user proficiencies, and unfamiliarity of security controls and processes within user areas, the integrity of information being generated by data processing systems for use by management, the board of directors, and the regulators should receive a sufficient level of review. Emphasis should be placed on the internal and/or external audit processes for reviewing and ensuring data integrity. Greater emphasis should be placed on evaluating sources and uses of data, critical computer applications, and the audit coverage afforded the integrity of critical information. If information integrity is not audited, then someone should sample and test key data and reports for accuracy on a periodic basis. As the

number of systems proliferate, so may errors and the potential for misleading if not fraudulent reporting. Thus, the decision-making processes resulting from critical information produced within the information systems environments may lead the organization to unsafe and/or unsound practices.

Output Controls

Whether displayed on a terminal monitor or on a report, visual access to sensitive information must be controlled. Within a financial institution or data processing center, there is a significant amount of information which is either printed and maintained in hardcopy format, stored and distributed via removable media (hard and floppy disks, tapes, etc.) or displayed visibly on CRT terminals and similar devices.

Written procedures for using system report generators need to be in place since users could query information they would otherwise have no process authority for. Additionally, any routine, pre-structured query instructions should be reviewed before authorization is given for their use and access to the instructions needs to be limited to ensure their integrity.

Sensitive data that is printed outside the data center or central computer room must require a specific action before the data is printed. Classified data must never be printed automatically to a remote printer. Once the report/data is released to the remote printer, the user must secure the output immediately.

Sensitive reports never should be left unattended by a copy or facsimile machine on an individual's desk. Classified information must be secured in a locked desk or cabinet to prevent the possibility of theft, unauthorized disclosure, or modification. Procedures must be developed for disposal of confidential data. For example, shredding machines could be available to destroy hardcopy reports. A degauser (magnet) can eliminate or destroy hard and floppy disks and tapes that contain confidential data.

Segregation of Duties

Segregation of duties is critical to the accuracy and integrity of data on any platform (mainframe, minicomputer, LAN, and PC). Security control measures must include the separation of duties for all computer operations. The separation of duties is used to prevent the perpetration of fraud by an individual. If duties are adequately separated, fraud only can be committed through collusion. It also is a detective safeguard, that is, the more people who are involved in processing, the greater the probability that fraud will be detected.

The following are examples of separation of duties:

- Require input transactions to be reviewed foraccuracy and legitimacy by someone who has not been involved in their preparation.

- Require adjustments and corrections of master records to be reviewed and approved by someone other than the person who approves routine transactions.

- Separate the functions which relate to the preparation and approval of input and those which relate to the distribution and reconcilement of output.

- The information processing function should be independent of the user departments for which it processes information. Information processing personnel must be prohibited from initiating or authorizing any changes to applications, system software, master records, or other types of information stored on the system other than those required to effect recovery from processing failures

The PC user often performs all of the following duties: programming, testing, documentation, computer operation, input preparation, and reconcilements. In a traditional mainframe environment, each of these functions is performed by different individuals. This provides a more secure system. Segregating duties in PC operations is difficult and not always feasible. Consequently, compensating controls such as strict supervision of the conformance to policies and procedures and frequent review of input, output, reconcilements, as well as any changes to system software and applications are necessary.

As PC users gain expertise in the system, they become familiar with its security limitations. This knowledge could be an enticement to fraud. As a

preventive measure, cross-training, and mandatory vacations are recommended to assist management to detect evidence of illicit activity. Cross-training increases backup efficiency by creating a pool of individuals who can take over when the employee assigned to a particular function is unavailable, or has left the employ of the financial institution.

Segregation of duties also is critical in a network environment. For example, the person who makes changes to an application should not be the person who authorizes the change. In addition, much like the mainframe system, production and testing environments for application development and maintenance should be separate. All production work would come to a halt, if a user who is programming an application using the production files crashes the system. Finally, thorough testing must be completed before implementing software or an application to ensure data integrity, and operational feasibility.

TELECOMMUNICATIONS SECURITY AND ACCESS CONTROLS

Telecommunications or data communications is accessing a network or computer system from a non-direct link or remote location through satellite, radio microwave, or telephone line transmissions. Unauthorized dial-in access to mainframe, minicomputers, and LANs is a serious threat today. Precautions or control mechanisms must be in place to prevent threats to the financial institutions systems, applications, and data. Telecommunication controls generally are supplied for terminals, files and for data transmission. Many techniques used to control data communications systems are discussed in the following paragraphs.

Telecommunications Access Controls

Computers (terminals and PCs) have become a more common means of communication for programmers, internal user departments and customers. Additionally, the use of PCs and other types of intelligent terminals is expanding rapidly as costs decrease and software becomes more flexible and menu-driven. Controlled access becomes increasingly complex due to expanded computer capabilities, geographic dispersal of terminals and use of various communications paths. Security not only must address physical restrictions to the computers, but must also provide system controls by function, operator, transaction and data type.

Software security features, which may be an integral part of the operating system, provide proper identification of the user, terminal and transactions and apply constraints on when the network may be used. These features may include:

- Identification and authentication checks;
- Automatic call-back procedures.
- Authorized activity or function tests.
- Time of day control locks.
- Automatic timed log-off.
- Access exception reporting.
- Security logs.
- Management intervention (turning modem on/off).
- Encryption algorithms.
- Automatic log on ID suspension when the number of attempts at accessing the system have reached a specified limit.

The identification and authentication feature is a fundamental control. The system should identify and verify the user, the type, and location of the hardware, the date and time, the transactions attempted or performed and their status, and the data resources accessed. Users may be identified through any combination of techniques that include a unique identification code (often referred to as a personal identification number (PIN), encoded cards, badges, encryption or verification keys, physical traits (voice or fingerprints, etc.), or passwords. Passwords are the most commonly used identification control and authentication tool.

Identification and authentication of physical computers is especially important. Terminals and PCs are connected to the system by modems, dataphones, or acoustical-couplers attached to public or leased lines. Some computers can be identified by two levels of special identification numbers which are encoded internally. The lower level identifies the terminal or PC. The higher level provides transmission of a security code that is installed in tamper-proof circuitry to protect against the interchanging of computers. These numbers can be verified automatically against a protected table of valid identifiers maintained by the system.

Another technique used to validate computers after a user has signed on, is the call-back method, where the system disconnects the terminal or PC and reconnects the line to a valid address. For dial-up systems, phone numbers should be adequately protected and changed periodically.

In certain situations, institutions will allow installation of PCs at employees' homes, with access to the mainframe or PC-based LAN via modems. Provisions for close supervision of home use of PCs should be implemented by the security administrator. Strict policies must be established to govern such use, including:

- Senior management approval.
- Screening employees who have this privilege.
- Establishing separation procedures which provide for the return of the computer and invalidation of logical access privileges when employees are terminated (voluntary or involuntary).
- Limiting employee activities performed via dial-up mode.
- Prescribing disciplinary actions for violations.

Regardless of the location of the remote computer, all users should be subject to the same data security measures as are those in-house. Once a user has passed the identification/authentication process, access should be allowed only to authorized systems, information, transactions, and commands.

The extent of telecommunications security in an organization varies and depends on risks and costs. In each instance, the comprehensiveness and effectiveness of existing controls should be determined by carefully assessing the system's security risk and the potential effect to the financial institution.

TRANSMISSION CONTROLS

Special controls must be in place to protect the confidentiality and accuracy of transmitted data. The reliability of transmitted data may be improved by using telecommunications controls such as:

- Parity checks.
- Message Authentication.
- Encryption.
- Error checking transmission protocols.

Although satellite and radio microwave transmissions are used, telephone lines are the most common method of linking the remote user with a central processor be it a mainframe, minicomputer, or LAN server. Since telephone lines are not maintained exclusively by the data center, physical and procedural controls should be reviewed to determine that the system is both reliable and secure from outside penetration.

Essentially, two types of telephone lines may be used in a teleprocessing system: dedicated private (or leased) lines and dial-up (or switched) lines. Dedicated lines are devoted 100 to the transmission of data between the host computer and the end-user device. The consistent quality of transmission and improved security afforded by dedicated lines make them preferable to dial-up lines. However, the versatility and low cost of dial-up lines make them useful in many instances such as low volume, infrequent communications, or as a backup means of transmission should dedicated lines become inoperable. Two types of dial-up lines can be used: regular public telephone communication lines and hybrid systems that use leased lines not specifically dedicated to a private user.

While communication line penetration is not easy, data communication systems are susceptible to exposure from line penetration or interception. The penetrate a teleprocessing system depend on the perpetrator's technical knowledge of data communications, the vulnerability and accessibility to equipment. A telecommunications system is vulnerable to penetration or message interception through several methods:

- Masquerading – Pretending to be an authorized user or repair person to gain access to the system. Access to user identification and authentication codes (if they are in use) would be necessary.
- Eavesdropping – Tapping or cutting in on telecommunications transmissions to monitor messages without interfering with them. Access to identifiable communications lines or links

would be necessary.

- Piggybacking – Monitoring transmitted messages to intercept, modify or replace and then retransmit to the host computer or user. Line access is required for piggybacking. In addition, a perpetrator would need a terminal capable of interfacing with the penetrated telecommunications system.

- Between lines – Inserting a compatible terminal into the communications channel. The system is accessed whenever the authorized user is signed on but inactive.

- Line grabbing – Inserting a compatible terminal into the telecommunications line. The perpetrator eavesdrops on the line until the authorized user signs-off. The sign-off message is intercepted and prevented from reaching the host system. The user is sent a false sign-off acceptance message, thereby giving the perpetrator free access to the system.

It is not possible to physically secure the communications lines, particularly when satellite or radio microwave links are used. However, the following methods may be utilized to reduce the penetration and transmission exposures inherent in these systems:

- Restricting access to documentation describing system design and development and listing the locations of telephone equipment and related teleprocessing communication lines. In view of the highly vulnerable and sensitive nature of communications equipment, all non-authorized personnel should be identified and supervised properly while in its general vicinity. Additionally, the specific telephone lines dedicated to on-line processing might be left unmarked or unidentified to hinder wiretapping or intentional sabotage. Codes for identifying all communications links could be used; their inventory should be kept in a secure area.

- Encrypting all passwords and vital data transmitted over the system. Encryption enables the transmission of data or messages in a format that discourages or prevents using data gained by unauthorized interception. There are two types of encryption:

  - Reversible encryption occurs when the sending unit transforms the clear text into cipher text and the receiving unit decrypts the cipher text back into the original clear text.

  - Irreversible encryption involves only the transformation of clear text into cipher text. There is no procedure to decrypt. This is useful, for example, for the internal storage of PIN's. (Encryption is generally used whenever the transmission of data requires that it be protected against unauthorized disclosure and undetected modification. Data encryption generally protects a transmission from interception and de-encryption by all but the most sophisticated interloper.)

- Using authentication checks on all transmitted messages. This would provide the receiving station with assurances of message validity. A code is inserted into each message based upon a sequential number, calculation or an algorithm tied to the last previously authenticated message.

- Using communications specialists to inspect telephone closets or install detection devices using limited terminal polling to determine the existence of wiretaps.

- Serially numbering each transaction received from a terminal or PC with a unique identifier. In some instances, the numbering process includes the date and time of day.

- Using automatic disconnects. Any terminal or PC inactive for a predetermined time period is disconnected automatically from the computer system.

- Using time-of-day controls where access is restricted to specific authorized times. Access at any other time would require supervisory approval.

Data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programs or vital data are being transmitted, additional controls are needed. Transmission errors are controlled primarily by error detecting or correcting codes. The former are used more often because error correcting codes are costly to implement and are unable to correct all errors.

Generally, error detection methods such as a check bit and redundant transmission are adequate.

Redundancy checking is a common error detection routine. A transmitted block of data containing one or more records or messages is checked for number of characters or patterns of bits contained in it. If the numbers or patterns do not conform with predetermined parameters, the receiving device ignores the transmitted data and instructs the user to retransmit it.

Check bits are often added to the transmitted data by the telecommunications control unit (TCU) and may be applied either horizontally or vertically. These checks are similar to the parity checks normally applied to data characters within on-premises equipment. A parity check on a single character generally is referred to as a vertical or column check, and a parity check on all the equivalent bits is known as a horizontal, longitudinal, or row check. Use of both checks greatly improves the possibilities of detecting a transmission error, which may be missed when either of those checks are used alone. If only one parity check is used, a horizontal check is more effective, particularly when coupled with advanced character coding schemes.

The effectiveness of checking techniques in detecting data transmission distortions cannot be denied. If the capability for making these checks is not provided by the equipment manufacturer, they would be difficult to implement in-house. Therefore, error detecting techniques should be considered before making decisions regarding equipment purchases for teleprocessing networks.

COMPUTER VIRUSES

As networks have become commonplace and as PCs have proliferated, computer viruses have become a serious threat. Computer viruses have infected computer systems around the world and the threat is likely to continue.

Computer viruses are computer programs, unique in two respects: they can attach themselves to other computer programs, and they can replicate themselves and move to systems. These attributes are accomplished in such a way that the user may not realize the virus was even in the code until it becomes active. The virus may perform obvious actions (such as displaying a message) or may be more insidious by triggering entirely random actions (such as erasing parts of memory).

There are two types of computer virus, nondestructive and destructive. Nondestructive computer viruses usually take some kind of annoying action such as screen messages, screen blanking, changing monitor display colors, delaying execution of commands, etc. Destructive viruses, on the other hand, may partially or fully erase hard disk files and tables making them unusable or unrecoverable, do level formatting of disks, modify data files, suspend systems so they do not respond to keyboard entries, etc.

Computer viruses most often are encountered on networks and PCs. Due to the complexity of the operating system and the security on mainframe computers there have been very few cases of computer viruses on mainframe computers. However, with the increasing connectivity of computer networks and the trend toward more open systems, the threat of computer viruses is magnified. The fact that a virus can attach itself to code or messages that are transmitted over networks to unforeseen destinations, and that it can then replicate itself and begin the process all over again, means that an entire network, and the networks linked with it can be infected.

Virus Symptoms

Viruses can infect all PCs including those with DOS, UNIX, OS/2, and Macintosh operating systems. The following symptoms may indicate the presence of a computer virus:

- A program grows larger for no apparent reason.
- The number of bad sectors on hard disk suddenly increases.
- The appearance of icons changes inexplicably.
- The system freezes up or crashes.
- Available memory is filled up suddenly with trash, zeros, or other unexpected data making it unavailable.
- The hard disk accesses become more error prone (file not found messages).
- The disk drive light comes on when there is no known disk activity (saving a file, copying, etc.).
- The PC does not respond to the keyboard in a consistent manner.

Of course, many computer viruses let the victim know that they have indeed been a victim and either display a telltale message or quite visibly demonstrate that things are going astray. In such cases, there can be little doubt about virus infection. Other viruses wait for a predetermined event to occur such as a date. This is the case with the Friday the 13th virus and Michelangelo (March 3) birthday virus. If one of these is suspected, the system should be recovered with software from uninfected sources before the event or the computer date set ahead.

Controls

Viruses can infect a PC through public software (shareware) loaded from the floppy drive or through programs transmitted from public electronic bulletin boards. Therefore, one of the best ways to prevent computer viruses is not to allow them an entry into the PC.

Preventive controls are:

- Do not load computer programs from public electronic bulletin boards or other untrusted sources. If these must be used, load into an isolated computer until the programs can be adequately tested.
- Use diskless PCs if feasible.
- ALWAYS put write-protect tabs on original diskettes before loading into the computer for the first time. If the computer does not have a hard disk, always boot from a write-protected diskette.
- Viruses commonly attack the DOS COMMAND.COM file in the root directory. To protect it and other DOS software program files, make them READ ONLY by using the ATTRIB +R feature.
- Make backups on a regular basis, but be aware that even backups may be infected. Protect original disks and do not leave them in open areas.
- For networks, do not permit network users to access any outside bulletin boards (including the internet) without prior approval. Do not allow any transfer of executable programs over the network. This would also include connections from the internal network to the Internet.
- Virus scan all new or foreign diskettes before using on a PC, including newly purchased software.

Organizations should have a security policy which prohibits using untested or unlicensed software, loading software from bulletin boards, or using shareware that has not been validated. The policy also should prohibit copying of software and using personal software on the organization's PCs.

If computer viruses cannot be prevented, the next best line of defense are detective controls that detect the presence of a virus. There are a number of good antivirus software programs on the market which can detect the presence of various types of viruses. They can be run at the option of the user or be run automatically whenever the computer is powered up, the program can be executed by the AUTOEXEC.BAT file. The user should be cautioned that antivirus software should be periodically updated by the vendor in order to account for new viruses or new techniques.

Corrective controls are the final defense against computer viruses. Isolate any system that is suspect. Stop all processing on the system or network. The user should not attempt to replace infected programs and recover the systems. Special procedures should be predetermined and followed to isolate and recover from computer viruses.

There are special tools and utilities for recovery and restoring files (PC TOOLS, Norton Utilities, MacTools) without having to rebuild entirely from scratch. However, these should only be used by the expert user and not a novice to avoid even more damage. If in doubt, seek expert assistance.

Caution should be used before restoring from backup copies as they may also have the virus. There truly is no 100 percent safe method for virus protection, but vigilance and careful procedures will minimize the risk.

This section is intended to review compliance with established policy and procedures protecting or securing data and facilities that process and maintain the organization's vital information. The effectiveness of physical security and data security plans, policies, and procedures should be assessed. The examiner should document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

Tier I

SECURITY ADMINISTRATION AND ACCOUNTABILITY

1. Determine if an overall security administrator has been appointed. Review the role of the security administrator and/or information security personnel to determine their familiarity with the organization's overall security policies and whether they have adequate authority to recommend and implement controls.

2. Review policies and procedures within the security administration function and whether they provide adequate separation of duties and appropriate supervisory review of security system maintenance activities.

3. Determine whether senior management is involved in and supportive of the information security program.

SECURITY PLAN

4. Review the data security plan and/or policy and assess its adequacy.

5. Determine whether the security plan for the IS operation is compatible with the security plan of the entire organization.

6. Determine whether procedures are in place to update the security plan and/or policy.

USER EDUCATION

7. Determine if an education program has been implemented to promote user awareness about organization's security policies and procedures and

assess the adequacy of the training program and materials.

8. Determine whether employees certify periodically as to their understanding and awareness of the information security program.

PHYSICAL, BUILDING AND CABINET AND VAULT SECURITY

9. Assess the building's security program and describe the equipment and/or other measures the data facility uses to provide protection.

PHYSICAL SECURITY FOR PCS AND DISTRIBUTED DATA PROCESSING ENVIRONMENTS

10. Describe and evaluate physical security for standalone PCs and distributed data processing environments (e.g., LANs).

11. Determine whether management has based the level of security measures of standalone PCs or other distributed data processing environments (e.g., LANs) on the significance of the applications processed and the potential risks and exposure to the organization?

PERSONNEL, DATA FILE MEDIA, AND COMPUTER OPERATIONS SECURITY

12. Assess the adequacy of physical and operational controls for the computer operations area including:

    a. Computer room security.

    b. Personnel safety.

13. Determine whether there are adequate safeguards and procedures in effect to ensure that only authorized persons are permitted in the computer or machine areas and tape/disk file library.

HARDWARE AND SOFTWARE INVENTORY

14. Identify and describe the authority ordering and distribution of hardware and software if not centralized describe the process.

15. Determine if an inventory system is used to record hardware purchase, distribution, and disposal and assess its adequacy.

16. Determine if all software (whether purchased or developed in-house) is accounted for through an inventory system and its assess its adequacy of the inventory system.

DATA AND PROGRAM SECURITY

17. Describe and assess the adequacy of controls over:

    a. Operating system commands, programs, and utilities.

    b. Application system source and object programs and utilities.

    c. Development and test programs.

    d. On-line functions, transactions and data.

18. Identify whether levels of access are approved and periodically reviewed by management.

19. Identify whether procedures are in place to address personnel transfers, new hires, and terminations.

TELECOMMUNICATIONS SECURITY AND ACCESS CONTROLS

20. Describe the types of telecommunications systems used and assess their security features.

TRANSMISSIONS CONTROLS

21. Determine if controls are in place to protect the confidentiality and accuracy of transmitted data (e.g., parity checks, message authentication, encryption, etc.).

COMPUTER VIRUSES

22. Identify and describe the measures management has taken to prevent corruption of data or software and to correct problems caused by computer viruses.

CONCLUSIONS

23. Review the results of work performed in this section and in sections for planning, audit, and management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

24. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

25. Assign rating (see Chapter 5 for additional information.)

26. Prepare an index of workpapers for this section of the workprogram.

27. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

28. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner	**Date**

Reviewer's Initials

Tier II

SECURITY PLAN

1. Determine if the security procedures covers:

    a. Physical protection of the data processing facility.

    b. Designation and duties of the security officer(s).

    c. Authorized data and program access levels.

    d. Requirements for password composition and change procedures.

    e. Requirements for access via terminals, modems, or computer system interconnection.

    f. Monitoring and follow-up of security violations.

    g. LAN and PC security requirements.

2. Determine whether updates to the policy and procedures are distributed to and reviewed by all appropriate personnel in a timely manner.

PHYSICAL, BUILDING AND CABINET AND VAULT SECURITY

3. Determine whether physical security in the data processing operation is coordinated with that of other organization functions.

4. Determine whether visitors to secured areas are required to sign-in and wear proper ID for easy identification.

DATA AND PROGRAM SECURITY

5. Determine how the security system operates and:

    a. How access levels are granted.

    b. Whether all access is restricted unless specifically authorized.

    c. If the password file is controlled (e.g., encryption).

    d. How security violations are detected and reported.

e. Who maintains the system and whether there is proper segregation of duties.

f. If reports of security file maintenance are reviewed by an individual without maintenance duties.

6. Determine that access levels are commensurate with job assignments, including whether:

   a. Data entry is separate from file maintenance.

   b. File maintenance is performed at a supervisory level or receives documented supervisory review.

   c. Individual users are restricted to application files and functions relative to their job responsibility.

7. Assess whether passwords, user ID's and encryption key procedures are adequately controlled for:

   a. The assignment of passwords.

   b. Changing passwords and ID's on a regular and frequent basis.

   c. Suppressing passwords and ID's on the video screen and all printed output.

8. Determine whether passwords are required to be alphanumeric or in some other format that is difficult to guess.

9. In a distributed data processing environment, determine whether controls are in place to limit opportunities to transform the data as it moves through various systems.

10. Determine whether sensitive data is adequately controlled (e.g., printouts, removable media, data visible on CRT terminals).

11. Evaluate whether do security control measures include adequate segregation of duties.

TELECOMMUNICATIONS SECURITY AND ACCESS CONTROLS

12. Determine whether physical access to system terminals is appropriately controlled by:

a. Terminal locks.

b. A physically secure location.

13. Determine if logical access to system terminals is controlled appropriately by:

a. User identification.

b. Automatic call-back procedures.

c. Automatic time-out or log-off.

d. Time of day control locks.

e. Terminal identification and authentication checks.

f. Access exception reporting.

g. Security logs.

h. Encryption algorithms.

i. Automatic logon ID suspension when the number of attempts at accessing the system have reached a specified limit.

14. Determine whether terminals are controlled as to:

a. What files they can access.

b. What transactions they can initiate.

15. Assess whether dial-up phone numbers changed periodically.

16. Assess whether dial-up lines are controlled by either an automatic callback procedure or physical connection (manual intercept) by operations personnel at the data facility.

17. Determine whether reports are generated that record:

a. Unusual activity.

b. Unsuccessful attempts to gain access to the teleprocessing system or applications.

c. Teleprocessing network problems/statistics.

	Comments
18. Determine whether exception reports are reviewed regularly by management or data security personnel for follow-up action.	

COMPUTER VIRUSES

19. Identify the frequency with which virus identification programs are run and updated.	
20. Proceed to Tier I Conclusions.	

Examiner	**Date**
_____	_____

Reviewer's Initials

NETWORKING - CLIENT/SERVER CHAPTER 15

(FILE NAME ON DISK # 2 = S2C15.WPD)

A technology revolution has been taking place in the computer industry in recent years and it is expected to continue well into the future. It concerns the use of the PC, its power, its speed, and connecting that power into networks. The use of networked systems brings about a new set of concepts needed to understand network operations and controls to reduce its vulnerability.

To view a system only as its components can blur its process of operation. The following definitions may help to understand that process.

A **computer communication system** is a system composed of data communication links and nodes that create a tool for the exchange of information among the attached components. This includes hardware and software that may be an integral part of the computer system, a separate entity, such as a communication service or any combination of user-supplied components.

A **data communication network** is a system of communication links consisting of modems, multiplexors, concentrators, front-end processors, data matrix switches, monitoring and control/management equipment, and various leased and switched terrestrial and satellite transmission facilities. They are organized and into a network using standard hardware interfaces, software protocols, and specialized network control applications packages to transmit information from one source to another. It is designed to meet a set of specific goals and requirements over a specified life cycle.

A **network architecture** comprises the functions performed by the network and the interfaces structure, and protocols used to perform them.

System components are connected to one another to form a network. The functioning of the network's architecture must be studied because it is the backbone of a network examination. The user should consider that:

- The examination should limit the scope of the process by eliminating application software from the review. An application software review can best be evaluated in the comprehensive or special examination.
- The cable (or whatever the medium of transmission) is a conduit to the functionality of the process.
- The workstation, computer, modem, printer, router, and bridge must be considered for the functionality of the components in the process of moving bits and bytes through the input to output processes.
- To examine a network it must be understood. There are many ways to portray a network. Few network drawings exist that truly represent the network's functionality.

The basic concepts of a network design are:

- *Layering* – The idea of a network is based on the concept of hierarchical layering. The communication mechanism is built one layer upon another, each one adding functions and capabilities.
- *Peer Layer Protocols* – Communication and synchronization between the distributed parts of a layer.
- *Multiplexing* – The sharing of messages among physical channels, seeking, and selecting a path for a message.
- *Topological Considerations* – Particular characteristics of specialized topologies; e.g., STAR, RING, and BUS.

NETWORK ARCHITECTURE/COMPONENTS

A network is a series of points connected by type of communication channel. The points (nodes) typically include a computer, switching equipment, printers, FAX machines, modems, and other devices.

Topology can be thought of as the shape or the way that the various individual parts of the network are connected for example:

Star Configuration

In a star configuration, all of the workstations are connected to one central system server. In this configuration the central process server controls all of the actions of the network nodes, and communication is processed through the central server. (Figure 15.1)

Ring Configuration

In a ring configuration, each workstation performs some of the services of a server device, and a workstation creates an action to be processed by the system. That action is passed (down the wire) to the next workstation until it reaches the appropriate workstation. (Figure 15.2)

Bus Configuration

In a bus configuration, all of the workstations are connected in a string-like configuration. The difference between the bus and the ring is that a ring has no terminal end whereas the bus has a defined beginning and end. A terminator is usually installed at both ends of the bus. (Figure 15.3)

LOGICAL MODELS

Logical models are conceptual representations of communication links and cables, transmission and switching equipment, and software which allow computers to communicate with each other.

ISO Open System Interconnection (ISO OSI) Model

In an effort to standardize the structure for interconnected computer systems and exchanging information, the Open System Interconnection Model was developed. This model is a foundation for coordinating computer interconnection "standards." The model is a layered hierarchical structure of communicating peer-to-peer protocols. The model defines the functions of each of the "standard" layers, the interfaces between layers, and the protocols used for peer communications. The model is based on the concept of communicating workstations. Components of the layers are described as follows (Figure 15.4):

- *Layer 7 – Application* – User-level and application-specific services and procedures. Distributed applications, information manipulation, resource management, virtual file management, etc.

Figure 15.1
Star Configuration

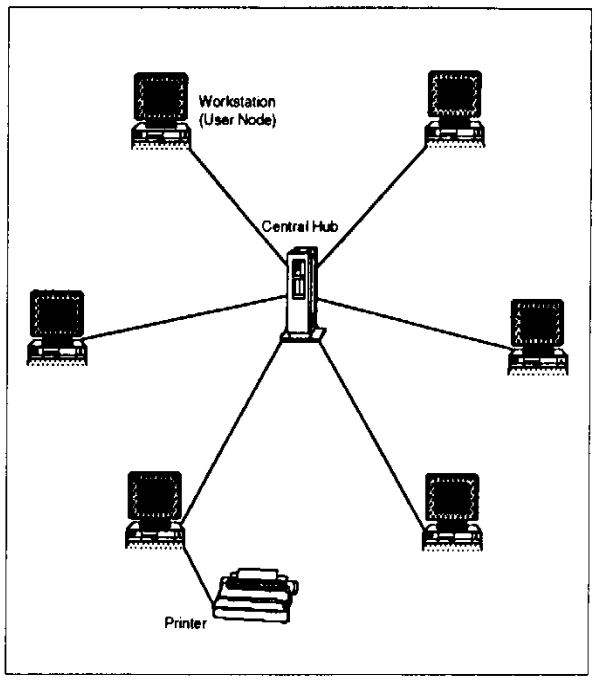


Figure 15.2
Ring Configuration

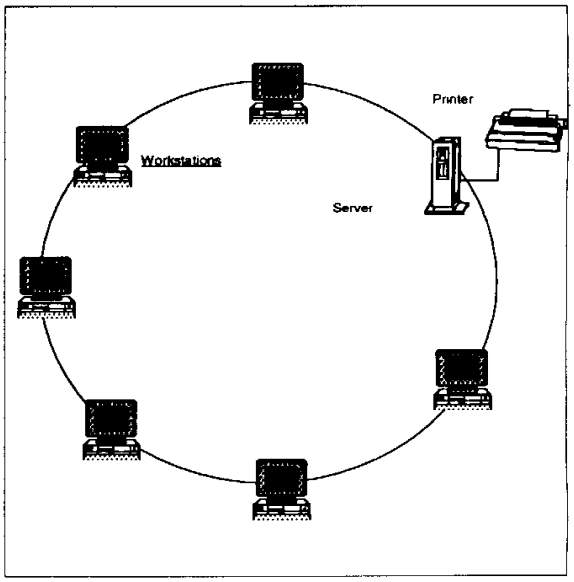


Figure 15.3
Bus Configuration

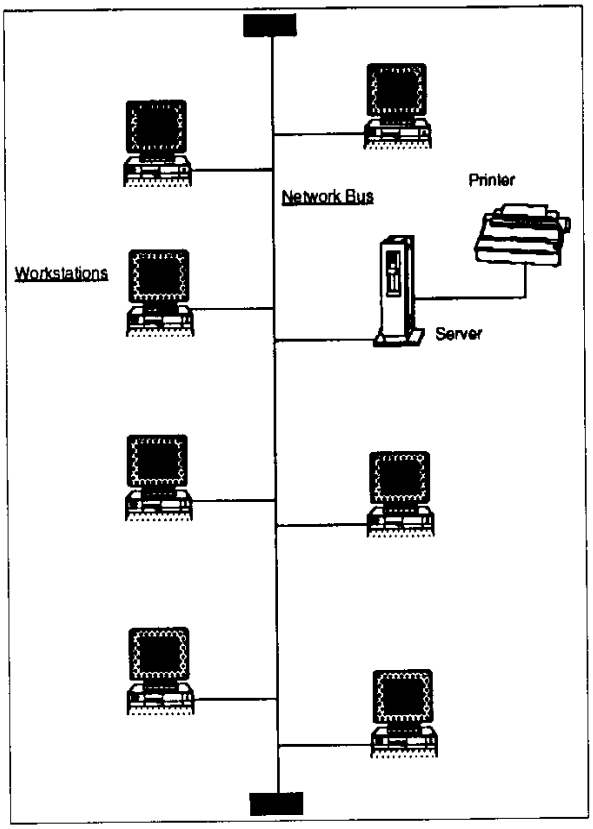
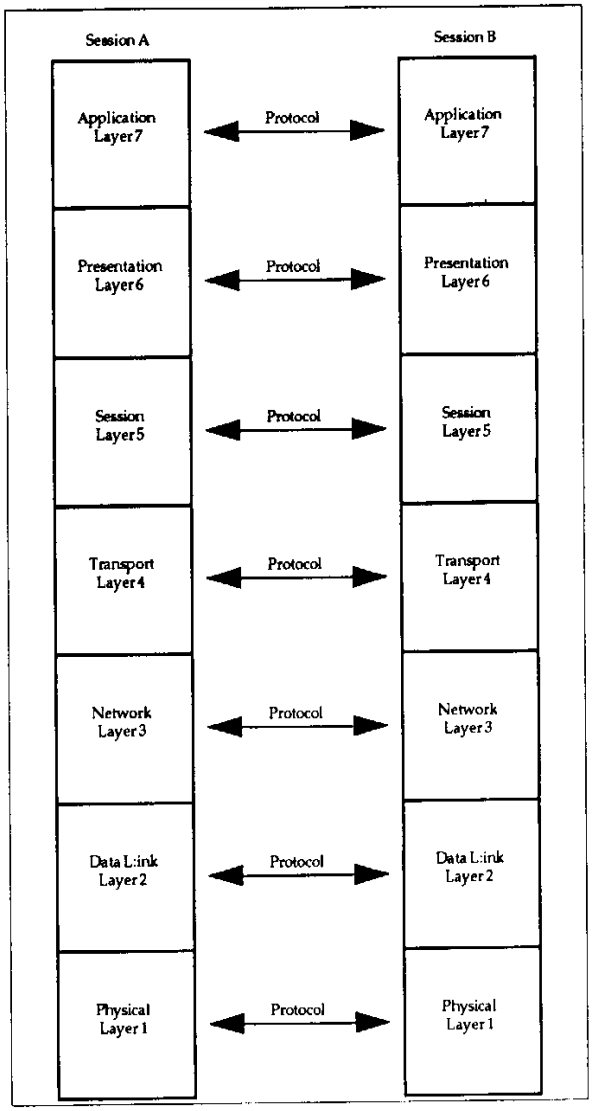


Figure 15.4
ISO Logical Model Open System Interconnection



- *Layer 6 – Presentation* – Representation of information, formats, codes, transformation, encryption, etc.

- *Layer 5 – Session Management* – Conversation initiation, initial screening, access security checking; synchronization, and abnormal recovery.

- *Layer 4 – Transport* – Sending messages. End-to-end control through (possibly multiple) networks. Packet assembly/disassembly (PAD); virtual circuit management, multiplexing, sequencing, message error checking, flow control.

- *Layer 3 – Network* – Sending packets or streams. Network management; routing switching, congestion control; initiating and end-to-end pathway.

- *Layer 2 – Data Link* – Sending blocks/frames. Link management; framing into transmission blocks; synchronization, bit error detection/ correction.

- *Layer 1 – Physical* – Sending bits. Functional and procedural interface to the medium; activate, maintain, deactivate the physical connection; modem control, etc.

- *Layer 0 – Physical Medium* – The medium that carries the energy that carries the information. Electrical/optical/mechanical specifications are

considered part of the medium.

Layers 1-3 form the transport or network service. Layer 4 serves as the liaison between the end system and network. Layers 5-7 reflect the end-user system.

IBM SNA – System Network Architecture

The IBM SNA model was introduced in 1974 by IBM. IBM had to migrate existing telecommunications users to SNA, which was evolutionary not revolutionary. This was done to make the network transparent to the users so they would not see the topology, route selection and media and to mask peculiarities of end-users virtual devices. The network was tailored to the specific needs of the users via selectable services. The SNA network provides a communication capability between logical representations of devices and applications.

The OSI model compliments the SNA architecture and each can supplement the other to provide a balanced solution for the management of networks and for the transfer of information between them.

The Consultative Committee on International Telegraph and Telephone's (CCITT) *X.nn* and *V.nn* standards recommend how particular electrical connections should be carried out.

- *X.nn Series Standards* – These are concerned with the connection of digital equipment to public data networks that employ digital signaling.

  X.25 is a standard that describes the interface between terminals operating in the packet mode on public data networks. It is known popularly as the X.25 gateway.

- *V.nn Series Standards* – These are concerned with the connection of digital equipment to a public telephone system that uses analog signaling. There are a number of V.nn standards that relate to public telephone system networks, each with its own set of standard guidelines.

- **LU6.2:** A new part of IBM's SNA is an Advanced Program-to-Program Communication (APPC). APPC is referred to by its two components, logical unit 6.2 (LU6.2) and physical unit 2.1 (PU2.1). IBM describes APPC as a program interface and an operating system. LU6.2 provides a set of conversion verbs that programmers can embed in a program when it needs to communicate with another application, such as to access a database.

OTHER PROTOCOLS AND STANDARDS

Transmission Control Protocol/Internet Protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) is the oldest networking standard that was originally developed for military communications. It has been made widely available, especially by its incorporation into the Berkeley Standard Distribution (BSD) release of UNIX. Today, it is implemented on operating systems and available from different vendors. Since each vendor implements its TCP/IP code differently, functionality will vary among vendors.

Synchronous Data Link Control

Synchronous Data Link Control (SDLC) is similar to the X.25. The SDLC protocol begins and ends each frame with a special bit pattern, known as a beginning and ending flag. The beginning flag references the position of the address and control frame elements and initiates error-checking procedures. The ending flag terminates the error-checking procedures.

Token ring networks are used in technical and office environments. Their principle of operation is that whenever a workstation wishes to send a frame, it first waits for a token. On receipt of the token, it initiates the transmission of the frame, which includes the address of the intended recipient. The frame is repeated (that is, each bit is received and retransmitted) by all workstations in the ring, until it circulates back to the initiating workstation, where it is removed. In addition to repeating the frame, the intended recipient retains a copy of it and indicates that this was done by setting the response bits at the end of the frame.

Carrier Sense Multiple Access Collision Detection

The Carrier Sense Multiple Access Collision Detection (CSMA) Ethernet protocol eliminates the collision of messages interfering with each other. If a collision is detected during transmission, the message is held back until some random time interval after the colliding message disappears. Although this does not eliminate collisions completely, it makes

them manageable.

DATA TRANSMISSION

The PC as a workstation in a network must have a means of transmission. As data leaves the workstation and begins traveling through the network, it requires a consistent method of transmission over the communication circuits/channels. Binary data can be sent over communication circuits in either parallel or serial modes by use of asynchronous, synchronous, or isochronous transmission methodologies.

Serial Mode

Serial is the primary mode of transferring information in data communications. Serial transmission implies that a stream of data is sent over a communication circuit in a bit-by-bit method. (Figure 15.5)

Figure 15.5
Serial Mode Transfer Circuit

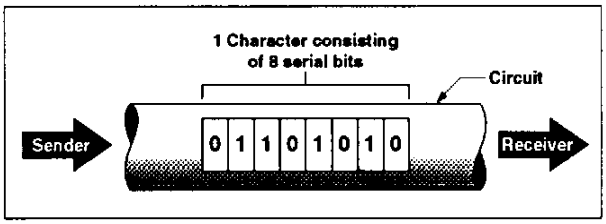
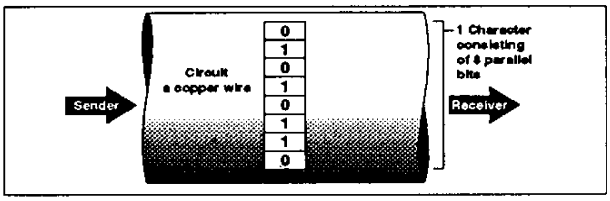


Figure 15.6
Parallel Mode Transfer Circuit



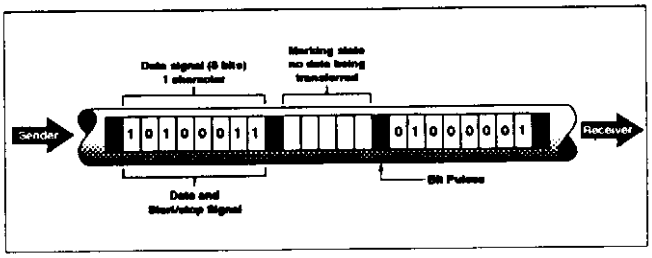
Parallel Mode

Transfers binary data as an *n-bit* all within the same cycle. In other words, if the internal structure of the computer uses an 8-bit element, all eight bits are transferred between the main memory and any operational register within the same computer cycle. More powerful computers use 32 bits. (Figure 15.6)

Asynchronous transmission

For asynchronous transmission, each character must have both a start bit and a stop bit.

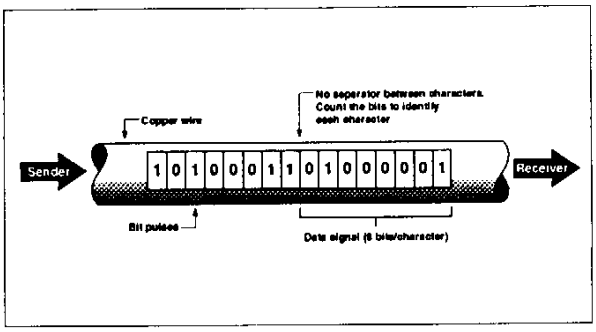
Figure 15.7
Asynchronous Transmission Circuit



Synchronous Data Transmission

For synchronous data transmission, the transmitter and receiver are synchronized. The synchronization time interval between successive bits is specified to an even multiple of the length of one code bit.

Figure 15.8
Synchronous Data Transmission Circuit



Special Devices

- *Modem* – Acronym for modulator/demodulator. It is a device that allows digital data (such as binary output data) to be transmitted, received, and understood over an analog circuit (e.g., voice telephone circuit).

- *Channel service unit (CSU)* – Allows digital data to be transmitted over a digital circuit.

- *Multiplexer* – A device that allows two or more users to share a common physical transmission medium.
- *Encryption* – A ciphering device modifies a signal to make it undecipherable while the signal is on the circuit of the network. A deciphering device is needed at the termination end of the circuit network to make the signal understandable (decryption).

HOST COMPUTER COMPONENTS

Network Operating Systems

The Network Operating Systems (NOS) is the functional heart of the network. Users generally think of the network as central operating software that defines its logical layout and oversees the allocation of its hardware, software, and peripheral resources. The NOS reaches into the physical network as its protocol. Although NOS is far removed from the physical topology of the network, an important relationship exists between it and the underling topology.

From a strategic perspective, it is the services offered by a particular NOS – the applications with which it is comparable, its tools for interconnection and connectivity, its management and its administrative resources – that often comprise the key factors in designing a LAN. The NOS has a direct affect on the topology chosen for the network.

UNIX

UNIX is an operating system that facilitates telecommunications and networks, but its acceptance has been slow in the commercial sectors. In 1988 AT&T and Sun Microsystems made a major investment and effort to make UNIX a foundation system. While it had the necessary functionality for communications, UNIX has not been widely used in business because of its lack of user-friendliness, business application, operating system facilities (security, file management), and on-line transaction processing. Those problems are being resolved, and UNIX may be increasingly accepted as a mainstream commercial operating system for business applications. UNIX has become one of the most widely used operating systems today. It provides multitasking, multiuser, heterogenous, computing environment on hardware platforms ranging from mainframes to PCS.

The primary feature of UNIX is its ability to provide application portability. Portability allows free movement of applications between dissimilar operating systems without having to recreate application interfaces. UNIX advantages include the ability to: support multitasking and multiuser environments; support multiple DOS sessions; allow mapping of UNIX and DOS disks to one another; allow DOS applications to act as clients to the UNIX-based file server; provide a platform for distributed systems computers in client/server

Telecommunications Access Method

Telecommunications Access Method (TCAM) replaces and extends both BTAM and QTAM (BTAM, or Basic Telecommunications Access Method, provides the basic functions to control data communication circuits. QTAM, or Queued Telecommunications Access Method, is an extension of BTAM that includes all of the BTAM facilities but will not support synchronous communications. See Chapter 31: Glossary for additional information). TCAM resides in the host computer. The most significant features are those used for network control and system recovery.

Virtual Telecommunications Access Method

Virtual Telecommunications Access Method (VTAM) is data communication software that complements IBM's advanced hardware and software. It resides in the host computer. VTAM manages a network structure based on SNA principles. It directs the transmission of data between application programs in the host computer and the components of the data communications network.

EXTERNAL CONNECTIONS

Gateway

A gateway connects two dissimilar networks, including two different communication architectures, and operates at layer seven of the OSI model. Gateways are associated with LANs and translate one network protocol into another, convert data formats, and open sessions between application programs.

Bridge

A bridge is designed to increase the number of addressable nodes on a network or to link two geographically distant, but similar, networks that use the same protocol. When two network segments are bridged, all traffic on either segment will pass on the other segment.

Routers

Routers join two networks that may be similar. The network segments joined by the router do not necessarily need to be of the same type: a router can connect an Ethernet to a Token Ring and to a public X.25 data network.

A router distinguishes data packets according to their protocol type and forwards traffic according to the logical or protocol address (rather than the hardware addresses that are used by a bridge).

Repeaters

Repeaters are simple devices that pass all traffic in both directions between the LAN segments they link. Repeaters are not discriminating. They are hardware devices that relay all they receive. A repeater extends the distance over which a network can be operated.

COMMUNICATIONS MEDIA AND CARRIERS

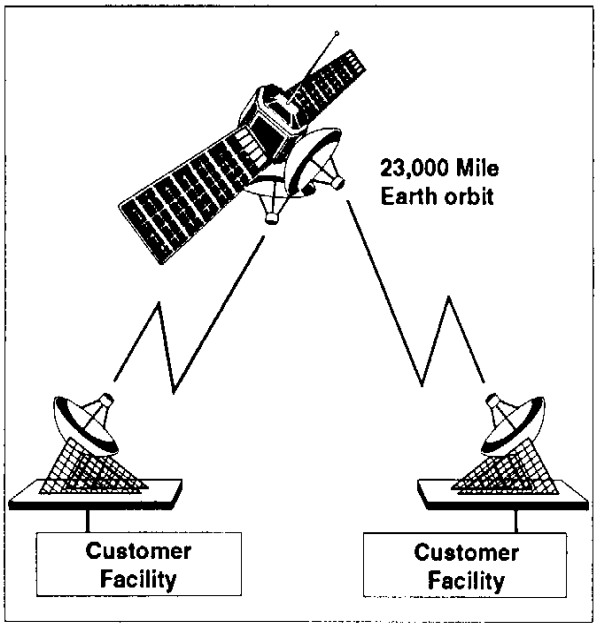
All communicated messages are carried by a type of medium. Communications carriers may be as common as a voice telephone system, or more specialized than public mailbox services and may be located on the LAN. The media may be arranged so that different network configurations and the components can be provided by specialized carriers.

- **Copper wire** is the most common metallic conductor for transmitting signals; it is used by telephone companies. Cabling connections with copper wire are made using standard jacks. Twisted wire pair is a form of copper wires used in the transmission circuits. Paired cable can be a few wires or several thousand twisted pairs.

- **Coaxial cable** is copper and sometimes aluminum wires bundled together to provide band-width transmissions of analog or digital signals. Insulated coaxial cable can be buried, run under water, or laid throughout a building on walls, ceilings, and floors.
- **Fiber optics** cable is composed of micro-thin fibers, usually glass, that use light energy rather than electrical energy. Information is transmitted as pulses of highly focused light. Fiber optic cable can carry a broad bandwidth with low signal degradation in less space than copper or coaxial cable. Fiber optic cable is more difficult to tap than copper or coaxial cable. Fiber optics cable also is immune to environmental conditions.

- **Satellite** communication begins at an earth station, passes through a satellite in geosynchronous orbit above the earth, and ends at one or more earth stations. The satellite serves as an active relay, and its communications relay systems, consisting of transponders and antennas, are its most important components. (Figure 15.9)

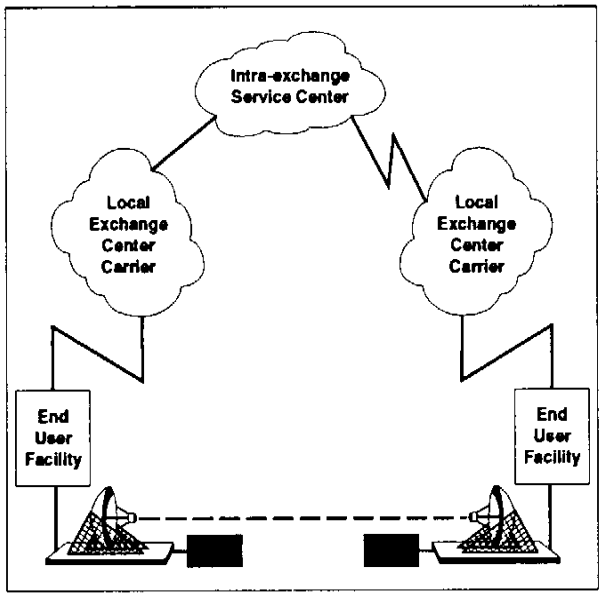
Figure 15.9
Satellite Services Configuration



These systems receive end-user transmissions from sending earth stations, amplify them, and retransmit them to receiving earth stations. The signal at the transmitter is much stronger than the one at the receiver. Since simultaneous signals at the same frequency interfere with one another, the satellite converts the signal it receives to another frequency before transmission.

- **Microwave** communication describes point-to-point radio. Microwave communications was once the domain of common carriers, but it has become a major competitor of standard, wire-line telephone communications. Microwave communications involves sending waves of information between a radio transmitter and a radio receiver, each generally mounted on a tower. It requires a clear line-of-sight. There can be no obstructions in the path of the transmitting and receiving antennas. (Figure 15.10)

Figure 15.10
Microwave Communications



NETWORK CONFIGURATIONS

Local Area Network

A local area network (LAN) is a data communication system that connects intelligent computer devices and peripherals and software, so that they can communicate and share resources, such as storage devices, programs, and data files. It integrates a wide range of functions into a single system. LANs are generally fault tolerant, incorporating a simple architecture with control distributed among participating stations. Since the entire network does not depend on a single polling or switching device, the failure of one component does not bring down the entire LAN.

Metropolitan Area Network

Metropolitan area networks (MANs) generally include several locations within a single metropolitan area.

Wide Area Network

When computers are located in different cities, public-carrier facilities must be used again. This network is known as a wide area network (WAN). The type of WAN used will depend on the nature of the application. This means that a WAN can span the globe.

The use of high-capacity communication lines, coupled with standard transmission protocols, over long distances provides the capability to tie geographically diverse processors or multiple vendors into a single environment. The processors on this network can be accessed equally by any user, providing that appropriate communications software is available to the user on either a microcomputer that emulates a network-attached terminal or on a mainframe that the user is able to access.

Value Added Network

Value added networks (VANs) are constructed with leased lines (circuits) and serve many customers in different geographical areas. Usually they are general purpose computer networks similar to the ones developed by public companies, such as Telenet, Tymnet, US Sprint, and MCI. These VAN carriers transmit either data or voice. A VAN is designed to allow a large number of users to use the network for a fee, usually based on the time spent on the network or the volume of data transmitted.

The VAN is a good alternative when volume or traffic requirements are low, or when an organization is not prepared to maintain and manage a private network, or when special services, such as mailboxes are required. The VAN adds the risk of the service provider to that of the using organization.

Client/Server

Client/server computing is an application of cooperative processing in which a programmable workstation executes a portion of the application.

This type of computing allows an application to be divided into logical components that can be distributed among several connected devices.

Client/server is characterized generally by the division of an application into components processed on different networked computers. The client/server is made up of two distinguishable entities: a client, which requests a service or information from a server; and a server, which processes the request, performs the service, and returns the requested information to the client. The client/server model has the following capabilities:

- The client and the server can interact seamlessly.
- The client and the server are located on separate platforms and are connected by the network.
- The server can serve multiple clients concurrently and, conversely, a client can access multiple servers.
- The client or the server can be upgraded individually.

Applications, based on the client/server model of computing, provide a great latitude in deploying application functionality across the network. This flexibility enables the use of desktop and portable devices, which, when working with high-power, low-cost servers, helps provide a cost-effective business solution. The client/server supports customers making the transition from transaction-based processes to business-event and knowledge-based solution. This transition is accomplished by new technology enablers, such as graphical user interfaces (GUIs), multimedia, and imaging, on an enterprise level.

Standards are a crucial element in client/server architectures, defining the interface between clients and servers and ensuring client application portability, interoperability, and maintainability.

The immature nature of client/server architectures is a concern of the client/server system. Organizations are often forced to choose among proprietary approaches that may not be the most effective approach for the institution.

The following fundamental attributes are associated with the client/server architecture:

- A many-to-many relationship exists between clients and servers. One server can support multiple clients at the same time, and one client can access multiple servers at the same time.
- A server in turn becomes a client to another server. A server can change roles depending on whether it provides resources to a client or requests resources from another server.
- Clients and servers can be, and usually are, replicated throughout the network.
- Requests for servers are initiated by clients. Servers cannot initiate requests to clients.

Peer-to-Peer Network

This type of network gives every microcomputer access to all nodes of the network's resources. In a network of peers, any microcomputer can share its hard disk and printer with any other microcomputer. The network's users create names for their local printers and disk volumes and designate them as sharable network resources. Unlike server-based networks, peer-to-peer networks allow shared resources attached to any microcomputer without going through an intermediary, such as a central microcomputer server.

MANAGEMENT OF NETWORKS

As networks become larger and more complicated, tools must be provided for their management. Originally, such tools were needed only for managing WANs, since the long-haul lines were quite expensive and problems needed to be detected and fixed immediately, usually from a central location.

Today, the network system is an integral part of most organizations' communications infrastructure. Problems affect many or all users quickly and visibly. These changes have increased the scope of network management to cover the management of applications, so that the total effort is called systems management. There is little difference in control concepts necessary to manage systems and networks.

Network management requires mechanisms to define and monitor control information. Some systems, such as Novell's NetWare Management System (NMS), allow the area network administrator to

manage the NetWare LANs and attached devices that are spread throughout the enterprise-wide network. The basic functions of NMS include network fault detection, performance, configuration, security, and accounting management.

Change Management

Change management is a process to control changes in the system so that changes are properly developed, tested, documented, and approved. The concept is similar to the mainframe process, wherein a user requests a change to the network configuration, access level, and authorization. All changes should be well documented and follow standard change management procedures.

Ideally, two environments should exist in the system, a test and a production environment. Software should be tested off line. A test and acceptance plan should be developed and executed. The movement of the test system to production should be carried out using procedures and controls similar to mainframe software production change controls.

Failure Diagnosis

Analyzers are generally considered test sets that allow operators to simulate specific message streams to test devices, communication circuits, or other workstations. Analyzers fall into several categories, which include a protocol analyzer, response time analyzer, and data line monitor. Generally, however, these tools perform the same basic tasks.

An analyzer measures the responses of all hardware in the network. This equipment can determine whether the network meets its performance specifications. These devices detect the content (bits) of a frame or packet during its transmission. For example, it might measure poll-to-poll time, which is the time from the detection of the poll being sent to the terminal, until the time that the poll is again sent to the same terminal. Another could be the measurement of poll or response time. A protocol analyzer also can trap information when certain character sequences appear on the send or receive communication network. Performance response time and link utilization can be captured by some analyzers. Protocol analyzers, response time analyzers, and data line monitors tend to look like a portable microcomputer with a few extra switches and buttons on the front panel.

These devices are, active and passive. Active analyzers/monitors can generate data that are interactive on the circuit and can emulate various terminals because they are programmable. Passive analyzers/monitors merely monitor and collect data to be examined later.

A typical analyzer can monitor data, trap and count data for gathering communication circuit statistics, offer a video screen and printer, poll various stations, offer various protocols, possess breakout box capabilities, etc. It is possible to turn a microcomputer into a combined protocol analyzer, response time analyzer, data line monitor, and Bit-Error Rate Tester (BERT). It requires a PC adapter board, software, and external RS232 interface that can tap into the data line.

Response Time

Most telecommunications network users perceive that the quality of a network's service has a direct relationship to application response time. Poor response time is perceived to be poor quality performance. In reality, application response time is attributable to several factors independent of the network. The network plays a critical role in response time in a poorly designed network, and unnecessarily degrades the response time of its applications. In addition to overloading the network, other sources of poor network response time are line quality, equipment failures, and incorrect software initialization options.

Operations Management

Network availability is vital in an environment where on-line transaction processing applications are critical to the organization. Operational management controls help ensure that the network adequately supports critical applications. Operations management is the day-to-day management of the network. Reactive operations management responds to critical problems. Some general functions of operations management are:

- Making the network available to all users.

- Monitoring network status.
- Reacting to network alerts and alarms.
- Taking immediate, corrective actions to reroute traffic or move to backup equipment in order to increase network user availability.
- Responding to risks of network viruses and other network attacks by implementing appropriate software controls and a viable recovery plan.

Administration

Within a network environment, the network administrator serves many functions. A network administrator would:

- Monitor network efficiency statistics.
- Ensure that all files considered essential are periodically backed up and stored off-site.
- Establish and maintain adequate virus protection facilities on the network.
- Maintain a set of current security tables off-site.
- Reviewing network activity reports.
- Ensuring a source for certified network components exists.

Network Accounting Systems

Accounting management tracks costs associated with network usage. Network accounting systems can be an automated tool to control costs. This type of accounting can provide the ability to:

- Record outgoing calls by station, extension, or account code (for client or customer chargeback).
- Report usage.
- Control operational decisions, such as routing, duration times, and priority.
- Allocate charges for equipment and overhead.

A network accounting system also can provide users with the ability to:

- Identify misuse and abuse of the services.
- Bill telephone time and expenses.
- Allocate costs by department, etc.
- Select the most efficient and economical long-distance telephone networks.

The use of these accounting records enables management to identify fraudulent network use. There are many evolving control-related techniques available as network security controls. A few examples are:

- Time-of-day logging.
- Unusual requests reporting.
- Repeated efforts, etc. (look for anomalies).
- Encourage internal clocks with telephone call-back features.

COMMERCIAL NETWORK SERVICES

The number and range of products and services, including network technologies and vendor choices, resulted from the deregulation of the telephone industry in 1984. That process created a new set of services and providers. Service and installation problems have become more difficult because of the number of different interfaces available. The emphasis is now on competitive pricing (generally thought of as rate information) and cost control.

Because of deregulation, the local operating companies offer services other than communication circuits. These include office automation equipment, multiplexers, switchboards (PBX), modems, cellular mobile equipment, etc. They may become a major manufacturer as well as a seller/distributor in the near future.

The service area of each of the seven Bell Operating Companies is broken into local access transport areas (LATA). These LATAs can offer their own service, but must offer service to other, suppliers including AT&T, MCI, and US Sprint.

The LATAs have created a point of presence (POP). The POP is usually the end office to which the local loop is connected, so that messages can be sent on the

long-distance circuit when it leaves the local LATA. AT&T, MCI, and US Sprint have at least one POP in each LATA.

Public data networks, also called public timesharing networks and remote computing services, are available for virtually any data processing application, business function, or information retrieval service that might be desired. They are generally accessed through a subscription service. An organization may use the PDN to access low volume users and/or particularly remote location users. The PDNs ordinarily use dial-up and low-speed voice-grade lines.

Dial-up (Switched) Networks

Dial-up networks provide services through shared switching and transmission facilities. A switched network design assumes that not all users will use the network at the same time and provides alternate paths to increase the probability of call completion. A switched public network may not be able to handle call volume at peak times and can cause delays.

Leased Line (also called Dedicated or Nonswitched Networks)

These are usually private networks that use leased lines between two or more points to keep the line available. Many organizations encrypt leased lines to prevent data disclosure when the risk warrants the cost and transmission overhead.

T Carrier Circuits

T carrier circuts are leased digital circuits with a transmission capacity of 1,544,000 bits per second that move over two pairs of wires. The T carrier system is the standard for interconnecting digital communications. It is a hierarchy of digital transmission and multiplexing standards, ranging from T-1 to T-4.

- *T-1 Circuit* – Any digital communication system operating at a synchronous data rate of 1,544,000 bits per second. Data can be transmitted over a T-1 circuit at speeds ranging from 56,000 to 1,544,000 bits per second. Digitized voice uses 64,000 bits per second. By digitizing voice signals and multiplexing them with time division multiplexing, T-1 circuits allow for 24 simultaneous voice channels.

- *Fractional T-1* – Offers portions of a 1,544,000-bit-per-second T-1 circuit for a fraction of its full cost. Users who use more transmission speed than voice grade can have digital service.

- *T-2 Circuit* – Can transmit at a rate of 6,312,000 bits per second. Basically, a T-2 circuit is a bundle of four T-1 circuits.

- *T-3 Circuit* – Allows transmission at a rate of 44,376,000 bits-per-second (usually referred to as a 45-megabits-per-second circuit). A T-3 circuit is a bundle of 28 T-1 circuits.

- *T-4 Circuit* – Transmits at a rate of 274,176,000 bits per second. This is equal to the bandwidth of 178 T-1 circuits.

MISCELLANEOUS COMMUNICATIONS

Voice

To control voice calls, most business organizations install call management systems. These systems monitor telephone call traffic, point out peak periods, and track efficiency and other voice telephone communications. A hardware box that performs these functions can be installed to work with private branch exchange (PBX) switchboards. The PBX is a switchboard within which all of the telephone lines of an organization terminate. Usually several circuits from this switchboard go to the telephone company's end office. These circuits are generally referred to as trunk lines when devoted to voice and are called leased circuits, private circuits, or dedicated circuits for data transmissions.

Modern digital PBXs can use digital transmission switching techniques because they use 32-bit microprocessor chips that act as the central controller/central intelligence. A typical digital PBX uses a star architecture so that individual telephones or microcomputers can be connected directly to the central digital switchboard. Modern digital PBXs provide simultaneous transmission of voice and data.

A voice type circuit is an analog transmission. Therefore, digital signals passed over the analog circuit must be converted. This conversion is done

by a type of modem.

Communication services are supplied by AT&T, one or more of the seven regional Bell Operating Companies, MCI, US Sprint, General Telephone and Electronics (GTE), or one of the other common carriers.

Private circuit (lease) services are services leased from one of the common carriers. In other words, the private circuits are available for use by an organization 24 hours a day, 7 days a week, and charge a flat rate.

Measured use services are those for which charges are based on usage measured in time. In a Wide Area Telephone Service (WATS), a fixed monthly fee is charged for a number of circuit-hours used. If the time is exceeded, the rate or fee is increased. Some of the primary services in this group are direct dialing, WATS, 800/900 service, and packet switching.

Facsimile

The fax is a device that scans a document, converts it to digital data and transmits the digitized representation over the communication circuit. A like device is used to receive and translate the digitized image for printing. A fax uses a modem to transmit and receive the data. Current fax technology can be incorporated into both the send and receive functionality of a personal computer and/or LAN system.

In contrast to the low bandwidth available with a connection through an analog-switched telephone network, the usable bandwidth of a coaxial cable can be much higher. This potentially high bandwidth can be used in one of two ways. In a baseband single-channel mode, all of the available bandwidth is used to drive a single high bit rate along the transmission path. In a broadband channel mode, the bandwidth is divided to derive a number of lower bandwidth subchannels on one cable.

In the baseband mode, the cable is used exclusively for the transmission of data between two systems, that is point-to-point, while in others the normally high bit rate transmission channel is time-shared by a number of systems, referred to as a multipoint or multidrop configuration.

In the broadband mode, multiple (independent and concurrent) transmission channels are derived from a single distribution cable, using a technique known as frequency-division multiplexing (FDM).

Integrated Services Digital Network

Integrated Services Digital Network (ISDN) is a leased service in which the common carrier offers a communication circuit with two 64,000-bits-per-second transmission channels and one 16,000-bits-per-second signaling channel. This is a high speed digital transmission service which can combine simultaneous voice conversations, data transmissions, and image transmissions can be combined. ISDN generally uses coaxial cable or microwave.

POLICIES AND PROCEDURES

Clearly, policies and procedures have been a main stay requirement in computer operations. With networks, they are no less important. Policies and procedures should assure that employees understand:

- The use of assets for management control.
- Procurement processes.
- Hardware and software operational controls.
- Protection and confidentiality of information.
- System development life cycle, change management, security, problem/incident reporting, and contingency planning.

NETWORK SECURITY

This section will, to a limited degree, provide a brief discussion of network security. For a more detailed reference on general security, refer to the Information Systems Security section in this handbook.

Network management must control the security of the network and the data stored and transmitted over it. The security is intended to prevent data loss and unauthorized access.

Physical Security

Management should prevent the unauthorized user

from physical access to network devices or the transmission media.

Logical Access Security

Logical access security controls are designed to prevent users from gaining unauthorized access to the network resources or applications.

Many networks now use satellite, microwave, or other transmission modes to exchange data and information. One method to safeguard the information transmitted is to encrypt the data.

User identification (ID) and passwords are common in computer networks. Although IDs and passwords are considered a good practice, controls and change procedures are necessary to guard against their vulnerability more effectively.

Passwords are the first line of defense against a breach to a network's security. Several restrictions can be placed on passwords to improve their effectiveness.
Minimum Password Length and Format. If a user is allowed to change the password, rules should govern the minimum character length of the selected password. There should be rules that prevent the use of easily guessed passwords (a simple rule may include forbidding common words and/or requiring that special characters be used as part of the password).

- *Forced Periodic Password Change*. Forcing periodic changes to passwords is an important component of password security. However, frequency of change also has a down-side in that users have difficulty remembering new passwords.

User time and location controls when employed properly will enhance security. The controls demand, transmission or session usage be limited to specific devices and specified times.

Switched ports are among the most vulnerable security points on a network. These allow dial-in and dial-out access. They are security risks, because they allow users with telephone terminals to access systems. Although call-back is a potential control, it is not necessarily the most effective, because of the call-forwarding capability of telephone circuits.

Transaction logs can be an important aspect of network security. Every login attempt should be logged. The logging control should include the date, time, user ID and password used, the location, and number of unsuccessful attempts made.

Computer viruses are executable computer programs that may propagate, using other programs as carriers. They sometimes modify themselves during or after replication. A virus performs unwanted functions on a computer. Some viruses perform simple annoying functions, while others erase or modify programs or critical data. Viruses are typically introduced into a network by floppy disks, and the network propagates them throughout the system (See Chapter 14 for additional information on information systems security).

DISASTER RECOVERY

The concept of disaster recovery and planning has long been understood in the mainframe computer environment. With the proliferation of networks, disaster recovery planning has become equally important to critical network operations. Like mainframe disaster recovery, networks need:

- Network disaster planning.
- Network backup procedures.

For additional information about disaster recovery (See Chapter 10: Corporate Contingency Planning for additional information).

LEGALLY ENFORCEABLE STANDARDS

Legally enforceable standards provide criminal punishment for three types of computer criminals: those who gain access to federal computers; those who gain unauthorized access to computers at financial institutions that are covered by federal laws; and those who gain access to computers that hold national security data. Many states have additional laws on computer communications security in order to supplement and/or enhance the following federal statutes:

- *Federal Wiretap Stature of 1968* protects voice communications from interception.
- *Electronic Communications Privacy Act of 1986*

makes it a federal crime to intercept electronic communications, such as data communications or electronic mail, or to tamper with computers in a data network. This law also includes the intentional transmission or distribution of unauthorized software that damages computer data, software, or hardware.

- *Computer Fraud and Abuse Act of 1986* expands the jurisdiction of computer crimes to include those involving the private sector computers located in two or more states. The law also addresses the so-called private bulletin board systems that exchange computer passwords.

- *Computer Security Act of 1987* requires federal agencies to create information security standards.

- *Computer Virus Eradication Act of 1988* was created to fight the spread of computer viruses. The law prohibits programs for computers, or a computer itself, or information or commands that may cause loss, expense, or risk to the health or welfare of the user organization. The law also bans giving such programs to others.

RISKS AND CONTROLS

Risks

Application systems are available to network users through the telecommunications architecture. The controls required of the network will depend on the type of applications available on the network and the business the network supports.

Risks include the unauthorized access of confidential data, the unauthorized modification of data, business interruption, and incomplete and inaccurate data. Some examples include:

- The loss of network availability that may have a serious, perhaps a financial impact, on the business or service.

- Obsolescence of the network components, including hardware, software, communications, etc.

- Unauthorized and indiscriminate use of synchronous and asynchronous modems to connect to the network to other networks.

- Connection of the network to public switched telephone networks.

- Inaccurate, unauthorized, and unapproved changes to systems.

- Performance thresholds that do not isolate problems, including system faults, inventories, an audit trail, and historical data record.

- Service degradation and delayed problem solution by vendors, leading to inconsistencies and incompatibilities among components of the network.

Controls

On-line interactive systems require specialized telecommunications controls. Some examples include:

- Physical network security that prevents accessing the network devices or transmission media.

- Logical access security to prevent unauthorized use of the network once physically connected.

- Keeping the telephone numbers of the in-house network confidential, using of tone suppression devices on all ports, limiting network availability using authorization and authentication mechanisms, limiting access by location, and monitoring failed logon attempts.

CLIENT/SERVER INTRODUCTION

Traditional information technology in financial institutions employed a large central computer system. Increasingly, financial institutions are employing client/server (C/S) technology to develop and deliver mission critical products and services. Client/server technology uses a network typically installed in a business unit, rather than a centralized computing facility.

Client/server technology enables business units to develop and deliver products and services to market much quicker than traditional legacy methods. The tradeoff is that controls over these systems are typically substandard to those associated with traditional systems. That is, the use of client/server technology, unless developed with a high level of controls, increases the level of transactional risk in the institution. The reason for the substandard level of controls is that business unit managers are typically not information systems technology professionals. Yet, these managers find themselves with the responsibility for making decisions on employing client/server technology to meet their business requirements. The boards of directors and senior management of financial institutions should be aware of their responsibility to address risks associated with client/server computing and to

encourage the development and implementation of sound policies, practices, or procedures and controls over client/server computing environments.

C/S BACKGROUND

The traditional approach to data processing for banking functions has been to develop and use large mainframe or midrange systems which are expensive to acquire and maintain. These systems require special physical environments and lengthy application development processes. Application developers have not always kept up with development requests that would allow financial institutions to provide faster delivery of services and products. End users, who need immediate solutions, have become frustrated with this traditional approach to data processing. This new technology is now available, at a perceived cost savings, that could satisfy end user demand for more timely management information system solutions.

End user needs have led to increasing acquisitions of computers and commercial off-the-shelf programs by departments, business units, and individuals to reduce their dependence on a centralized data processing environment. However, this strategy has its own limits. For example, stand-alone computers make it difficult to share information with other information systems. This problem is being solved by the development of high-speed data transmission and network file servers in client/server computing.

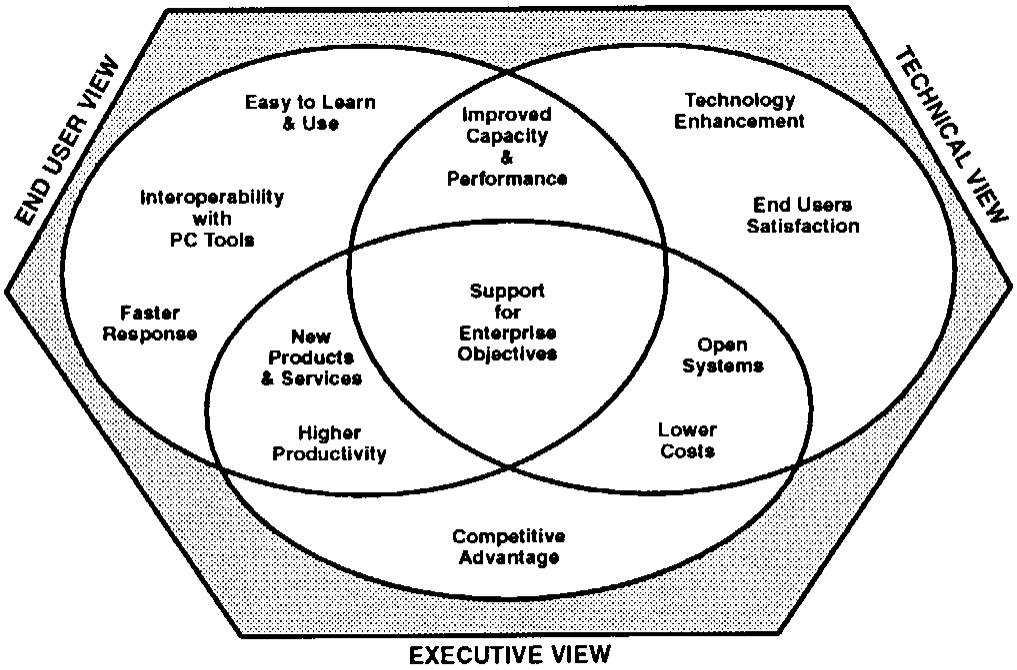
As a result, financial institutions are now processing mission-critical applications including funds transfer, branch automation, general ledger reporting, security portfolio accounting, and customer relationship management on client/server systems. Additionally, independent service providers (service bureaus) also are utilizing this new technology by providing these systems as part of their servicing operations to financial institutions. (Figure 15.11)

ROLE OF SENIOR MANAGEMENT

The board of directors of financial institutions must develop and adopt appropriate policies, practices, or procedures covering management's responsibilities and controls for all areas of client/server computing activities. Management must recognize that the implementation of controls is just as important in the client/server environment as in the mainframe environment. The institutions strategic planning should clearly define the technological and control architecture. End users and auditors must have a prominent role in the acquisition, development, and implementation of all client/server computing environments. (Figure 15.12)

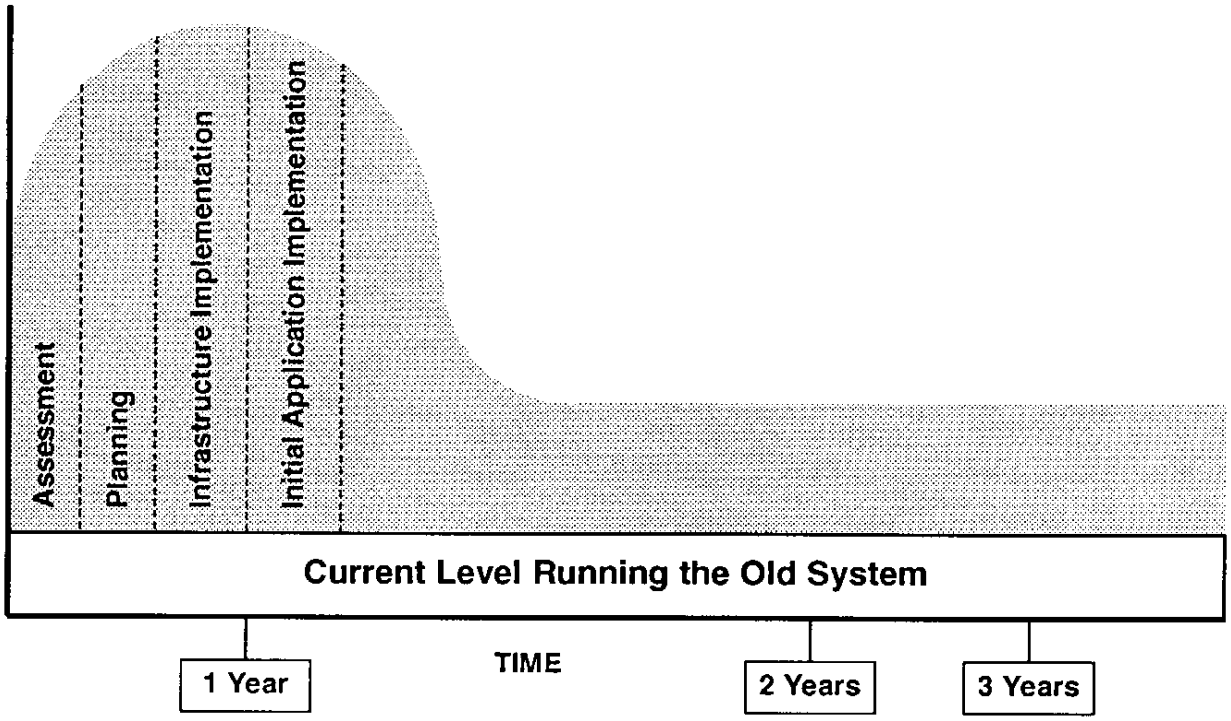
The existence of policies, practices, or procedures and the management supervision of client/server activities will be evaluated by examiners during regular supervisory reviews of the institution. See Chapter 25 and FFIEC SP-3: Joint Interagency Issuance on End-User Computing Risks for additional information.

Figure 15.11
Client/Server Can Be a Cohesive Force in the Enterprise Executive View



With Permission M. Zola Rapid Systems Solutions, Inc.

Figure 15.12
Client/Server Can Be a Cohesive Force in the Enterprise



With Permission M. Zola Rapid Systems Solutions, Inc.

DEFINITIONS

Client/server computing is a method of allocating data processing resources in a network so that computing power is distributed among workstations in the network. This type of computing allows integrated applications (general ledger, demand deposit accounting, loans, etc.) to share system and data resources using cooperative processing. Cooperative processing differs from traditional mainframe or distributed system processing in that each processing component is mutually dependent.

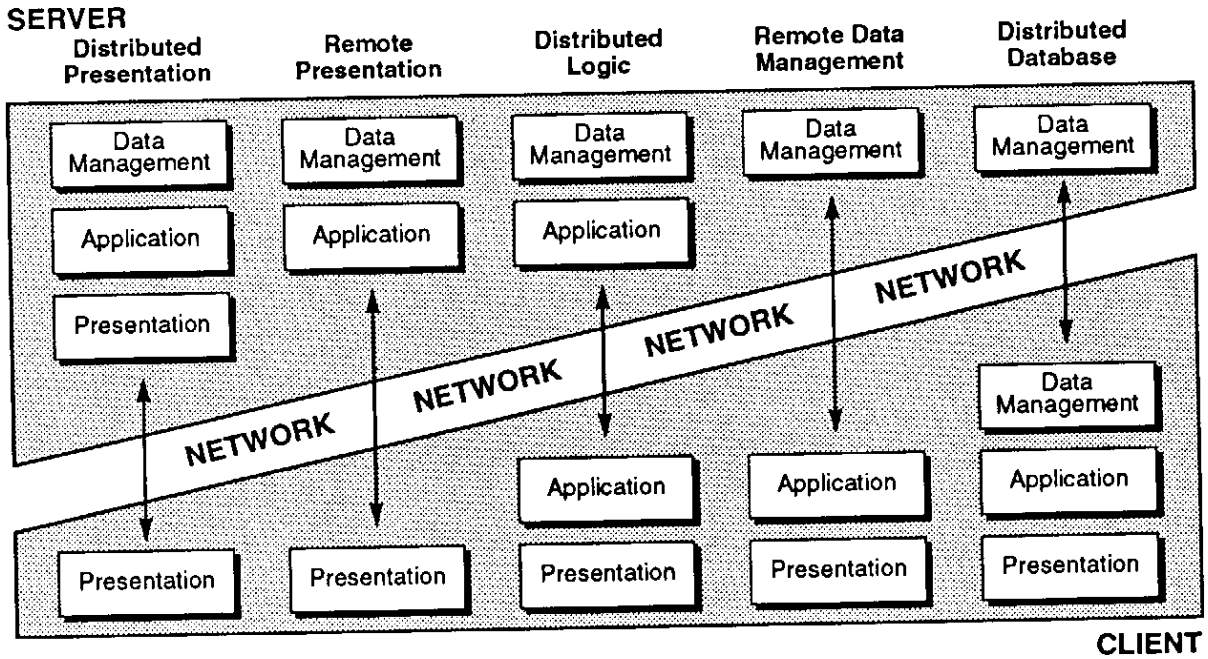
C/S COMPONENTS AND CHARACTERISTICS

- *Client* – A client (front-end) is a single PC or workstation associated with software that provides computer and presentation services as an interface to server computing resources. Presentation is usually provided by visually enhanced processing software known as a Graphical User Interface (GUI).

- *Server* – A server (back-end) is one or more multi-user computer, 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.

- *Middleware* – This is a client/server specific term used to describe a unique class of software employed by client/server applications. This software resides between an application and the network, and manages the interaction between the GUI front-end and data servers in the back- end. It facilitates the client/server connections over the network and allows client applications to access and update remote databases and mainframe files.

Figure 15.13
Types of Client/Server Computing



With Permission M. Zola Rapid Systems Solutions, Inc.

- *Distributed* – Most commonly, a server is a distinct computer that serves any number of client systems. It is feasible to have clients and servers on the same computer. The server may be in the same room as its clients, or it may be across town or around the world.

- *Decentralized* – Client/server systems are typically installed, administered, and operated by a business unit, rather than a centralized computing facility.

- *Complex* – Client/server systems usually involve multiple clusters of computers linked by high-speed communication lines. (Figure 15.13)

ISSUES AND RECOMMENDATIONS

The proliferation of client/server technology introduces new risks as well as benefits. In today's competitive environment, client/server technology can be a strategic initiative of the organization, and therefore is not just a technological concern, it is also a business concern. Customer demand for flexible and timely management information has fostered its growth. Faster delivery of services, ability to leverage emerging technology, autonomy of end users, and productivity gains from re-engineering the work flow are all potential benefits.

The client/server architecture has not evolved to the point where controls are inherent in the design, maintenance, and operation of the system. Controls are more difficult to implement effectively due to the distributed, decentralized and complex nature of the client/server environment. A prior section of this chapter illustrated some of the risks and controls that have been associated with network computing. These are also applicable to the client/server environment.

The need for controls over information systems environments is not new. What has changed is the control and decision making responsibility. Traditional or legacy systems were controlled

centrally. That is, most banks had large central computer resources with corresponding centralized software development resources. One of the reasons banks have migrated to the client/server technology is to reduce the lead time on bringing new products and services to market. This can happen very quickly in a client/server environment where the business unit rather than a central resource has control over the computer and software development resources. Unfortunately, not all business units have the software engineering expertise to develop systems with the high level of controls expected of bank information systems. With this decentralization of decision making over technology, larger banks can have literally thousands of client/server systems without any centralized management oversight or requirements for interoperability or compatibility.

Some of the control issues include logical access controls, i.e. controls which limit access to the banks computer systems and the activities performed once access is granted. Contingency planning is not always a consideration when developing these systems. For a mission critical system, lack of contingency planning could significantly impact the bank. Testing of the systems can be compromised in an effort to gain market presence. Accordingly, the cost of re-engineering can negate the anticipated savings of time and resources associated with a decision to implement client/server technology. Absence of controls over data base access through client/server systems could compromise the data base and the integrity of resulting management information.

This section is intended to determine the adequacy of the institutions controls over its networking operations. The levels of controls necessary will depend on the degree of reliance the institution places on its network operation. Systems could vary from small isolated LANs to worldwide networks using hardwired and/or vendor-serviced communications services. The networks should be reviewed in consideration of the importance of the information/data to the institution rather than the size of the network installation only. The examiner should document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

Tier I

NETWORK MANAGEMENT

1. If the institution is operating a LAN client/server operation and using a telecommunications system for information transport, describe the system(s) and associated user areas. Use a customer system diagram or create one and determine if the systems are:

   a. Hardwired local or remote client/server operations.

   b. Remote terminal operations using both local and remote client/server operations. Note the transport format including dial-up, leased lines, and value added and, public data networks, etc.

   c. Remote terminal operations using dial-up lines.

   d. Remote terminal operations having file transfer and/or processing capabilities.

   e. Remote client/server operations used for distributed processing and/or print/server operations.

2. Determine if key managers have an adequate segregation of duties and that their skills will enable them to perform their responsibilities.

3. Determine if networked operational systems are addressed adequately in disaster recovery/business contingency planning and testing. Assess the

perceived importance of these systems as compared with the contingency plans.

SECURITY

4. If the institution uses an on-line security system, assess its adequacy and effectiveness.

5. Determine if effective data security policy exists, and if it is being adhered to by:

   a. Discussing the deviations from the published and approved written security policy.

   b. Determining if there is a network security officer review and discussing his/her duties and responsibilities.

   c. Reviewing and determining the authorized access levels allowed within the network operation.

   d. Determining if a password change procedure exists and if it is effective

   e. Determining the composition of passwords (e.g., alphanumeric, nondictionary word validation, etc.).

   f. Determining who has the responsibility for maintaining of the security/password file(s).

   g. Determining whether security violations are monitored and tracked.

6. Arrange with internal audit, the network security officer, systems administrator, or user management to test access controls of selected systems (the examiner should not perform this test directly but rather observe it). Verify the security controls for sign-on, password usage, authorization, and authentification (i.e., read only, update, delete), and log-off. Review the security and/or activity logs that record security violations.

CONTROLS

7. Discuss the data entry controls at the point of origin. If data capture is also obtained through imaging, review – describe the process and associated controls.

Identify the controls in place over the data during input, processing and output activities.

8. If institution is doing any of its own application or systems programming, determine whether there are existing documented policies, procedures, or practices that describe application and systems programming control. Assess whether these procedures are used and are adequate to control new and modified application systems design, development, test, and implementation.

TRAINING

9. Determine whether there is an adequate technical training program for users, operators.

CONCLUSIONS

10. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

11. Discuss with management:

    a. Violations of law, rulings, regulations,or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

12. Assign rating (See Chapter 5 for additional information).

13. Prepare an index of workpapers for this section of the workprogram.

14. Prepare a separate summary findings worksheet for this section of the workprogram. The summary

should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

15. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

NETWORK MANAGEMENT

1. Obtain an official organization chart and staff position descriptions. Interview management *(*and staff*)* and identify the person(s) responsible for the daily operation of the network (usually the system administrator and security administrator). Determine if the person is qualified, and if there is segregation of duties between persons and any other tasks that they may be assigned/perform. Determine whether there is:

    a. A network system operations manager (sometimes referred to as a systems administrator).

    b. A network security officer (sometimes referred to as a security administrator).

    c. Another person(s) assigned who has specific roles in the control or operational area of the network (include those persons located at remote processing centers).

2. Determine whether system administration and operational procedures are documented and are current and:

    a. Whether the duties and responsibilities assigned to each position and function are clearly defined.

    b. The extent of separation of duties in key functions. Assess whether they are appropriate to the business risks associated with the functions and applications that reside on the system.

3. Determine whether there are written procedures and specific persons assigned, whose responsibilities include:

    a. Initial start-up instructions.

    b. Performance monitoring, operations, and usage.

c. Hardware malfunctions.

d. System security.

e. System maintenance.

f. Applications management.

4. Verify whether the department has current policies, procedures, and standards that are effectively communicated to appropriate personnel and addresses the following areas:

   a. Long- range (strategic) and short-range operating plans that are current and approved by management.

   b. Departmental and institutional policies and procedures.

   c. Each application being run on the network. For commercial applications, determine if there are sufficient license and/or application management controls in place.

   d. System operations procedures, including start-up, shutdown, system shadowing, mirroring, etc.

   e. Tape and/or electronic and optical disk management.

   f. Backup procedures, policies, and offsite storage.

   g. Emergency procedures.

   h. Stock paper and negotiable instrument control procedures.

   i. A contingency/disaster recovery program.

   j. Security procedures and an audit trail program.

5. Determine whether management has developed standards and proceduress defining the levels of information and applications to be classified as sensitive. Determine whether there is a definition of the differences between sensitive, critical, and shared data.

6. Determine whether management has identified the critical application systems.

7. Determine whether all policies, procedures, and control documents are signed/approved by management.

8. Determine if performance, audit, security, and problem reports are available to management and whether:

   a. They are reviewed by management.

   b. Action has been taken by management and, if so, the type of action.

9. Assess the adequacy of the physical and operational controls of the computer operations area, including access to:

   a. The network, client/servers, and the security, safety, and housekeeping areas of the system.

   b. The network communication system and the security, safety, and housekeeping areas of the component areas.

   c. The terminal devices and the security, safety, and housekeeping areas associated with each unit.

10. Determine the adequacy of controls over operator privilege activities and equipment operations.

11. Determine whether logs are maintained detailing hardware and software problems, and if these logs are reviewed by management.

12. Determine the adequacy of the procedures for reporting and logging equipment failures, maintenance, and repairs, and whether these log reports are reviewed by management.

13. Review the adequacy of reports used by management to monitor computer performance, utilization, and capacity.

14. Determine whether there are maintenance agreements covering all equipment and if not, what is excluded.

SYSTEM OPERATIONS CONTROLS

15. Determine whether procedures exist for problem resolution and:

    a. How they are tracked and their status reported.

    b. If appropriate escalation procedures exist to ensure appropriate response to system problems.

    c. Whether vendor responsibilities are documented in the problem management procedures.

16. Determine if there is a problem resolution log. Review the log and determine if:

    a. Problems recur often.

    b. Resolution timeframes meet management objectives.

    c. Problems represent a system control breakdown.

17. Check for the existence of system maintenance logs for network equipment and servers and determine whether the logs reflect:

    a. An adequate program of periodic preventive maintenance.

    b. Entries for performance capacity monitoring. If not, check to see if the system itself maintains a log.

18. Identify all system-generated logs. Determine if they are being used to track performance, capacity, and transmission quality and verify that procedures exist to:

    a. Periodically review the logs.

    b. Respond to system-identified problems or efficiency degradation.

DISASTER RECOVERY – BUSINESS RESUMPTION CONTINGENCY PLANNING

19. Determine if a written disaster recovery/business resumption contingency plan has been developed for the possible loss of the client/server network, and if it includes:

    a. Securing data files.

    b. Procedures for verifying levels of emergency or processing interruptions (e.g., short-term manual mode).

    c. System application recovery procedures.

    d. Remote storage of data, systems software, documentation, and the recovery plan.

    e. A list of documentation and files maintained offsite.

    f. Procedures to recover from a disaster, including hardware, software, and telecommunications failures.

    g. Provision for securing hardware and supplies.

    h. A location for the backup site.

    i. Approval of management.

20. Assess whether the disaster recovery/business resumption plan has been tested, in simulation, within the past year and:

    a. How often it is tested and how.

    b. Whether the results of the test are documented, and there has been, third-party monitoring of the tests.

21. Determine if policies or procedures exist to ensure the currency of the plan relative to system and/or application changes.

22. Perform an inventory of all items stored at the offsite location and determine the adequacy of the

facility, operation, and backup necessary to recreate files.

SECURITY

23. Verify the physical security provided for servers and communications networking equipment, and that:

    a. All servers are secured (preferably in an area inaccessible to all but authorized systems personnel). Describe how access is:

        - Authorized.

        - Controlled and monitored.

    b. Equipment is provided with physical locking devices or is otherwise properly secured. Determine whether:

        - Keys are properly secured, but accessible to authorized personnel.

        - Duplicate keys are stored and secured properly.

    c. Unrelated equipment and supplies are not stored in the secure area.

24. Verify that the physical security for network distribution equipment is adequate and that:

    a. All major, primary distribution equipment is in controlled access areas.

    b. For secondary distributed equipment (small clusters), it is protected from accidental disconnection or disturbance.

    c. For high risk application/operations, all distribution equipment is protected:

        - From unauthorized physical access.

        - From unauthorized monitoring by use of appropriate sheathing, conduit, or properly installed media.

- By procedures to detect and defeat unauthorized physical access to the distribution system.

d. All workstation distribution cabling and connections are installed properly and secured to prevent accidental disconnection or disturbance.

25. Determine if physical workstation security is adequate and how:

    a. Unauthorized removal of workstations and other equipment is prevented.

    b. Physical access is controlled and monitored for workstations and other equipment identified as sensitive or high risk.

26. Determine how physical access by vendors to network equipment is controlled and monitored including all equipment in questions 23 through 25 above.

27. Determine whether environmental conditions meet equipment specifications, including:

    a. Electrical supply, uninterrupted power supply (UPS) and emergency power and conditioning equipment.

    b. Heating ventilation air conditioning (HVAC) systems and controls.

    c. Static controls.

28. Determine that fire protection equipment is adequate and appropriate for the system.

29. Determine that fire protection/suppression for onsite stored media is adequate.

30. Determine if onsite storage of all system media is adequate to prevent unauthorized access, including:

    a. Server software and backup media.

    b. Workstation media.

31. Determine if access to printers and printed output is properly controlled and monitored and:

    a. What physical safeguards exist for sensitive printed output.

    b. What procedures exist for managing the physical distribution of printed output.

DATA SECURITY

32. Must all users on the network enter a logon ID and password to access the network server?

33. Are appropriate password and logon controls in force?

    a. Are the passwords displayed or hidden (nonclear) when they are entered?

    b. Are the passwords encrypted at the workstation before being sent to the server for verification?

    c. Does the system force the user to change passwords regularly? Describe the frequency of change?

    d. Are IDs automatically disabled by the system if passwords are not changed by users?

    e. Does the system prevent passwords from being reused, and are users prevented from changing back to previously used passwords?

    f. Are new users forced to enter a new password on initial logon (passwords pre-expired at first logon)?

    g. Is a minimum length password enforced by the system?

    h. Is there a system to authenticate and preview passwords to prevent common word/name usage (dictionary type password authentication prevention controls)?

i. Are passwords stored as clear text anywhere on the network, including the workstations or in the server?

j. Are user IDs automatically logged off the network after a period of inactivity?

k. Are group or shared IDs and passwords permitted on the network?

l. What compensating controls exist for the use of group or shared IDs and passwords?

m. Do employees sign a corporate systems policy statement acknowledging responsibility for confidentiality or information and secrecy for passwords?

n. Are users informed through guidelines and are they educated about security and establishing passwords

o. Are vendor, contractor, or temporary employee IDs set to pre-expire at the term of their contract?

p. Are vendors, contractors, or temporary employees restricted to appropriate logon days and times?

q. Are vendors, contractors, or temporary employees restricted to specific workstations?

r. Are vendors, contractors, or temporary employees required to sign appropriate nondisclosure statements regarding corporate information to which they may have access?

s. Are IDs disabled after several failed logon attempts? What is the frequency of failed attempts that disables the ID? How long are IDs disabled and how are they restored?

t. Are users notified of the number of prior invalid logon attempts each time they sign onto the system?

34. Are there password logon audit trails that show activity such as:

    a. Logons and logoffs (location, time, and user ID)?

    b. Type of access (dial-up, leased lines, public data networks (Internet, VAN, and etc.)?

    c. Invalid access attempts (location, date, time, ID)?

    d. System expired IDs?

    e. Logoffs due to inactivity?

35. Are audit trails maintained for a reasonable time?

    a. Are they reviewed?

    b. By whom, and how frequently?

    c. What action is taken?

36. Are exception reports produced from audit trails and reviewed by management?

37. Does the network software prevent access by unauthorized users to or from other network services (gateways, FAX, dial-out, WAN, etc.)?

38. Does the network software prevent access by unauthorized users to sensitive system functions such as Security Administration, network monitoring, server console operations, enabling/disabling services, etc.?

39. Are users granted access ONLY to disks, volumes, directories, and files for which they are specifically authorized?

40. Are users able to load and run ONLY those executables for which they are specifically authorized?

41. Identify all software security controls that are not integral to the network's operation system. Evaluate the effectiveness and verify that only

authorized persons can configure or defeat control features.

COMMUNICATIONS SECURITY

42. Determine if internal controls are adequate to prevent:

    a. Incomplete transmission.

    b. Misrouting.

    c. Unauthorized message alteration.

    d. Unauthorized disclosure.

    e. Message duplication.

43. Determine if communications security is built into the communications links on the network, including:

    a. Software packages.

    b. Encryption devices.

    c. Hardware features for the various servers and other processing devices.

44. If the network is connected to outside services or related services through the Internet determine if "firewalls" have been created to centralize access control to-and-from the network and the other service.

45. Determine how microcomputers are connected to each other and other processing entities including:

    a. Modems.

        - Direct dial-up
        - Dial-back.

    b. Hardwired (direct connect).

    c. Leased lines.

    d. Public data networks.

46. Review the adequacy and implementation of controls over the following communications hardware/software processing functions:

    a. Network change control.

    b. Dial-up access.

    c. Network activity logging.

    d. Data encryption.

47. Determine if controls are in place to ensure that data integrity is maintained during data transfer to or from the client/server and other processing entities and identify:

    a. The message authentication procedure.

    b. How the accuracy and completeness of a transmission assured.

    c. For data up and down loading, how batches are identified, screened, and approved on the network.

CONTROLS

48. Review, obtain, or prepare a list of all automated applications currently in use or under development for use on the network client/servers. Identify purchased applications (shrink-wrap and vendor custom contract developed) and those applications that were developed in-house (in-house and contract programmer). Also identify the party(s) responsible for providing maintenance support.

49. For vendor or contract programmer software supplied packages, determine that the following items can be provided by the network administrator. Review the following:

    a. License agreements.

        1. Number of authorized copies or users allowed (site license).

        2. Usage and costs.

b. Maintenance service agreements.

1. Vendor technical support.

2. Allowed modifications that can be made by the institution personnel.

c. User Documentation

1. User operating instructions.

2. Technical documentation.

d. Software acquisition and use policies.

CHANGE CONTROL

50. Determine if procedures exist for operations staff to manage change control.

51. Verify the following:

a. Does the program change process conforms to corporate program change control procedures and standards?

b. Is program change control for the network operation adequate?

c. Are the techniques used to monitor program change control adequate?

d. Does the systems change control procedures take into account the impact to the business, including system availability, user impact, system efficiency, and currency of documentation and manuals?

e. Are there adequate procedures to inform, train, and assist operations staff in the implementation and support of changes in the system.

52. Determine if procedures exist to inform and train users when system changes occur.

53. For network system and utilities, determine if the following are provided:

a. Maintenance information.

1) Technical support group that supports the product.

2) Provisions for receiving operating system fixes, enhancements, and upgrades.

3) Availability of manufacturer's direct support or alternative vendor support.

4) Contract or agreement governing maintenance procedures and services response availability.

b. User Documentation.

1) Is current technical and reference documentation available for operation, administration, and users of the network system software and utilities?

54. Determine if adequate test procedures exist for all changes to the system environment, including those to:

a. Test and implement operating system upgrades, patches, fixes, and enhancements.

b. Test and implement application upgrades, fixes, and enhancements.

c. Test and implement the introduction of new productivity tools and programs.

d. Test and implement changes in the physical environment.

55. Determine if an adequately configured test system exists with appropriate isolation to the "production" environment and:

a. If not, a logical test system exists. Do appropriate controls exist to prevent significant adverse impact to system efficiency or availability.

c. Specific procedures exist to guard against the introduction of “virus” or otherwise tainted executable programs in the test and production environments.

TRAINING AND USER EDUCATION

56. Are policies and procedures in place to ensure adequate technical training of the users, operators, and staff?

57. Does adequate documentation exist for use in training and as reference material for all system and application functions?

58. Are security and control concerns part of the education and training programs for the users, staff, and operators of the system?

59. How are corporate information systems policies communicated to personnel relative to training programs and materials?

60. How are changes to the system accounted for in training and education programs, including documentation and work aids?

61. Proceed to Tier I step 10.

Examiner | Date

_____|_____

Reviewer’s Initials

END-USER COMPUTING CHAPTER 16

(FILE NAME ON DISK # 2 = S2C16.WPD)

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.

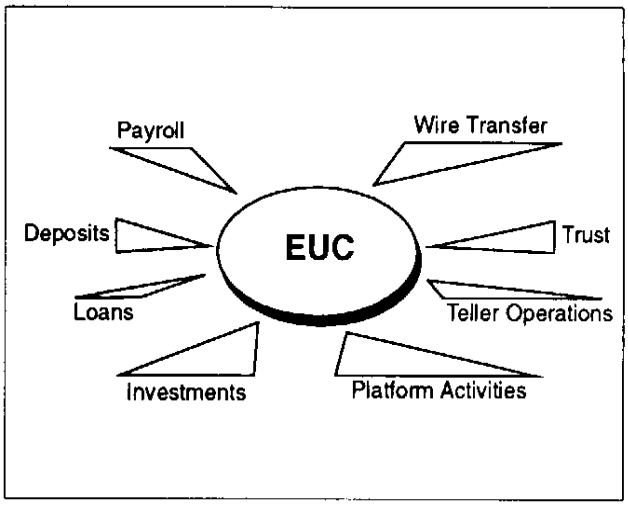
End-user computing is the transfer of information processing capabilities from centralized data centers onto the user's desktop. End-user computing systems may range in size and computing power from lap-top notebook computers, to standalone personal computers, client-server networks, or small systems with sufficient computing power to process applications for a financial institution. Small systems entirely supported by a hardware or software vendor are referred to as turnkey systems (not to be confused with PC/LAN systems). Control considerations discussed throughout this section generally apply to all end-user computing systems.

In many cases, end-user systems are linked in distributed processing networks. The ability to decentralize the data processing function is largely a result of the development of powerful microcomputers or PCs. Microcomputers are now powerful enough to process significant applications when used as stand-alone systems. These systems also can be connected to a host computer and configured to serve as data entry/display terminals. In this terminal emulation mode, information can be passed between the host and the PC with the processing occurring at either machine. Therefore, it is very important that controls over the downloading and uploading of data are in place and adequate.

Linking several microcomputers together and passing information between them is called networking. A system configured in this manner is commonly called a local area network (LAN). When linked by a network, end-user computing offers several advantages to financial institutions, including:

- Low cost relative to other platforms.
- Efficiency through the sharing of resources.
- Ease of expansion for future growth.
- Enhanced communication capabilities.
- Portability.
- Data availability.
- Ease of use.

Figure 16.1
End-User Computing Activities Overview



Although end-user computing systems provide several advantages, there are increased risks to data integrity and data security. These risks include:

- Difficulty in controlling access to the system.
- Lack of sophisticated software to assure security

and data integrity.

- Insufficient capabilities to establish audit trails.
- Inadequate program testing and documentation.
- Lack of segregation of duties.
- Inadequate System Development Life Cycle (SDLC) procedures.

As the trend toward distributed processing continues, financial institutions should have proper policies, procedures, and reporting to ensure the accurate and timely processing of information. The controls in an end-user computing environment should be no different from the those implemented in a traditional mainframe information system environment. In this new environment, local management and staff should assume responsibility for the information assets of the organization. Institutions that design reporting systems to fit their specific needs also have a competitive advantage.

CONCERNS

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 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.
- 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.
- Training.

Responsibilities for the acquisition, implementation and support of such networks should be clearly established (See Chapter 25 for additional information on FFIEC SP-3: Joint Interagency Issuance on End-User Computing Risks).

STANDARDS

Acquisition Criteria

The increased use of microcomputers, end-user computing platforms and microcomputer networks in financial institutions requires management to establish appropriate standards and policies governing

the acquisition, implementation, and support of end-user computing. Management should establish acquisition standards, for both hardware and software, as uncoordinated purchases could result in excessive costs, redundancy, incompatibility with other systems, and servicing complications. End-user computing acquisition policies may include:

- Feasibility studies at the user/management level.
- Development of a centralized purchasing unit.
- Corporate wide guidelines for user departments.

Microcomputer acquisition policies should eliminate duplication of effort by user departments and save money. However, new policies should be introduced carefully to user departments. Management should avoid cumbersome or inflexible policies that may be ignored by microcomputer purchasers. A set of balanced microcomputer acquisition policies should serve the needs of both management and users (SP-3: Joint Interagency Issuance on End-User Computing Risks).

User Standards

User standards and effective employee training programs are crucial to prudent microcomputer use. Although the microcomputer may not need a specialized temperature-controlled environment, there are other security considerations. For example, the microcomputer location should discourage unauthorized access and passwords should be required to access PC standalone and shared programs.

Standards relating to the microcomputer software process can help prevent and detect errors or the fraudulent manipulation of data. Misuse and inadvertent errors can erase programs and data on microcomputers resulting in serious problems. User standards should describe the risks involved in operating microcomputers. A well informed user should understand the need for controls and recognize that microcomputers contain sensitive data.

HARDWARE AND SOFTWARE SELECTION

Software selection may limit the institution's hardware alternatives. For example, some software is designed to operate on a specific group of computers or requires a hardware configuration that only can be supported by certain vendors. Before selecting hardware, a financial institution's management should prepare a list of requirements for comparing alternative hardware proposals.

The two most important considerations in selecting hardware are the machine's capacity and its performance capabilities. Evaluating capacity requires a review of the institution's present and future needs, including projected growth, types of automated applications, anticipated new products, and future management information requirements.

A decision also must be made whether to purchase or lease the equipment. This decision should consider the costs of each method, including the tax and earnings consequences, and the effect of technological advances on future hardware costs and performance. Although either method is acceptable, the decision to acquire a system should be made only after conducting a comprehensive review of the institution's present and future objectives within the context of its strategic plan. This should include systems compatibility and interconnectivity for future expansion purposes. In the absence of such a review, management might purchase an inefficient or inadequate computer system, which could result in a substantial loss if the equipment had to be sold or upgraded. Costs for hardware and software generally should be amortized over 4 to 7 years. Otherwise earnings may be misstated.

Software Selection

Selection of the right software for each business function is critical to overall microcomputer success. Because of the variety of software available for microcomputers, the following questions should be addressed in establishing software selection guidelines:

- What applications are to be processed?
- What is the appropriate use of licensed software?
- What access control mechanisms are included in the software?
- How should in-house developed software be controlled?

- How much user involvement is needed in selecting the software?

Senior institution management should be involved in establishing proper criteria for software purchases. Although microcomputer software is relatively inexpensive, it is an investment that benefits the organization. A commitment by management to establish comprehensive software selection criteria should help maximize the benefit of all software purchases.

Physical Protection

Financial institutions should protect the computer equipment. Because of their portability, microcomputers are especially at risk of being stolen or misused. The location of microcomputers and the types of applications being processed should determine the extent of physical security that is required. At a minimum, microcomputers should not be located in areas that afford easy access to customers or unauthorized employees. Whatever physical security the financial institution determines is appropriate, the effectiveness of the security measures depends on employee awareness, and management's enforcement of the controls.

Care also should be taken to shelter the equipment from environmental risks. For example, the microcomputer should not be placed under a sprinkler valve that can be triggered by a fire in another area of the building or in a flood-prone basement. Surge protection devices should be used to prevent damage due to fluctuations in power.

Every financial institution should have equipment to prevent fire damage. In a small institution, such equipment is often limited to portable fire extinguishers. The cost of a more extensive fire protection system, while desirable, may not be justified.

OPERATIONS

End-user computer operations is a microcosm of the traditional data processing center. Senior management should work with local managers to develop policies and standards for applications development, documentation, change controls, and security. Refer to the appropriate sections of this handbook for discussions of these topics.

A key element in maintaining a properly controlled operations environment is the segregation of duties between each area. However, small institutions may find that separation of duties is not practical because there are few employees. In such circumstances, it may be possible to establish an acceptable control environment by instituting compensating measures, such as the rotation of duties.

Important controls in end-user computer systems reside in the user departments. The person in the user department who initiates transactions should not be responsible for reviewing output and balancing reports. Audit trails should be provided for all posted transactions, including file maintenance. Transaction reports should be printed and made available for review. The need for the user departments' involvement in reviewing and balancing reports cannot be overemphasized. This is one of the best control mechanisms for an end-user system.

DISASTER RECOVERY/CONTINGENCY PLANNING

As end-user computer systems increase in computing power and processing capabilities, it is important to assess the adequacy of disaster recovery and contingency plans for these systems. The need for contingency planning is related to the importance of the applications being processed. Critical data maintained on Pcs must also be protected through proper back-up procedures. As financial institutions begin to process more critical applications on end-user systems, the contingency plans for these systems should become more closely aligned with those of larger systems.

Special consideration should be given to adequate back-up frequency for data files. Management often undervalues information on PCs and fails to implement proper back-up routines.

NETWORKS AND TELECOMMUNICATIONS

Financial institutions with microcomputers and other end-user computer systems rely on telecommunications to interconnect the organization's computing functions. Telecommunications allows users to communicate and share information and

resources. In decentralized processing, this type of communication is critical to assimilating information from various organizational units to use in the management decision-making process.

If the system is a LAN located within a single building, the risk from external sources, such as tapping telephone lines, is reduced. The primary concern is the adequacy of controls over the desk top functions and the type of information that can be accessed. These concerns usually can be addressed through the operating system software or by controls programmed into the applications software.

The capabilities of each end-user system and the controls present to protect the integrity of the financial data and software should be determined. Many systems will have activity logs that show user activity. If such logs are available, a knowledgeable supervisor should review them for unusual activity (See Chapter 15 for additional information on firewalls and other forms of hardware, software, and network controls).

SMALL SYSTEMS

In some financial institutions, end-user computing systems may include a large microcomputer or minicomputer with peripheral equipment that processes all applications for the institution and functions as a small data center. The hardware manufacturer or the software vendor may assume full responsibility for the system design and installation, and supply all necessary hardware, software, and documentation. This type of system is referred to as a turnkey system. Small system control considerations generally apply to all end-user computing systems.

Financial institutions with small systems may purchase or lease software packages to process such applications as demand, savings, and time deposits; loans; investments; and general ledger. In many cases, these software packages also include a central information file. Application software for turnkey systems is usually obtained from the hardware manufacturer or from an independent software vendor.

Vendor software generally consists of standardized programs. Customized enhancements may be available for additional charges, but may not be provided in a timely manner. Most standardized software packages offer a variety of options, including various user reports, account types, and interest rate and fee options. Such options are usually table-driven, giving an institution's staff the ability to change them without requiring programming changes.

When a financial institution acquires application software from a vendor, both parties will usually sign a software maintenance (including purchase or lease agreements) agreement. Under the agreement, the financial institution usually will be entitled to receive all new software releases, with installation and operation assistance provided by the vendor for a set fee. New releases may contain requested changes from users, modifications to comply with changing legal and regulatory requirements, or corrections to previous versions. Some software applications also may require annual maintenance updates. Releases may be provided according to a set schedule or issued only as needed. Some vendors will not provide programming support, unless the user has installed all of the previous releases. Therefore, a financial institution should remain current with software releases to ensure vendor programming support and compatibility with other users.

In financial institutions with little or no programming capabilities, emphasis in the selection process should be placed on the careful analysis of all available software packages that could include a cost/benefit feasibility study. Some key questions to consider include:

- Does the software meet the present and future needs of the institution?
- What reports and records does the institution need?
- Does the system include audit reports?
- Does it have a system log or an on-line log?
- Are there adequate program controls for data integrity?
- Does the software contain access control features such as password protection of various applications?

- How are the passwords generated, and can limitations be placed on their length and composition?
- Can the systems be configured to force periodic password changes?
- Are passwords stored in encrypted form?
- Is the software installed in other financial institutions?
  - If it is, visits to other institutions with a similar operation may be beneficial in evaluating the system.
  - If it is not, it may be more difficult to determine whether the software will meet the institution's needs, and backup arrangements may be more difficult. In such circumstances, extra care is required to ensure that the new software performs as expected before the conversion process is completed.
- What is the cost of the software?
- Is there an additional cost for executing the software at multiple workstations?
- Does the software vendor supply programming support?
  - If yes, at what cost?
  - If no, how will program problems be corrected?
- Is the vendor readily available to support the software?
- Does the vendor have the financial capacity to provide long-term support?
- Is the software documented?
- Does the financial institution receive or have the right to obtain source programs and program documentation?
- Does the institution have the right to modify the software?
  - If so, how does this affect the future warranty and vendor support?
  - If not, how does this affect plans for future operations?
- Do contracts for buying or using the software protect the rights of both parties?
- Is the software compatible with other computers?
- May it be used to service other institutions?
- Is the software easy to use?
- Are the operating and user guides adequate and are they written in clear, easy-to-understand language?
- Is adequate employee training provided?

Often, user groups are formed to address issues concerning a particular software package. Where possible, institutions should strongly consider joining such groups.

Program (System) Change Control

Many vendors request dial-up access to provide on-line programming support. While this method may assure that modifications are made in a timely and efficient manner, the financial institution is subject to the risk that the person who requests access over the telephone is not a bona fide vendor employee. In order to control this risk, a financial institution should implement a procedure, such as calling the vendor back at a predetermined number, to verify that the caller is an authorized vendor employee.

Any changes to application software by anyone other than the vendor may void warranties. As a general rule, in-house modifications should be made only at the direction of the vendor. If the modifications are vital to the institution and the vendor is unwilling or unable to make them within a reasonable time, senior management should be made aware of the problem and the potential ramifications of not making the modifications.

Third-party Escrow Agreements

Over the past few years, the software market has become extremely competitive, and many software vendors are concerned about the confidentiality of their programs. In order to retain more control over their products, some vendors prefer to give only

object programs (machine language programs) and user guides to their customers. Another method of maintaining confidentiality which allows the financial institution access to the documentation, is to establish a third-party escrow agreement. Under this arrangement, an escrow agent retains a copy of the source programs and supporting documentation in safekeeping with instructions to deliver the materials to users in the event the vendor is unwilling or financially unable to support the software.

Provisions that are usually incorporated into an escrow agreement include:

- A definition of acceptable software maintenance.
- Conditions that must be present before the customer can obtain the source programs and documentation.
- The media in which the source programs will be released; e.g., magnetic tape, disk, or hard copy.
- Arrangements for auditing the escrow arrangement.
- An assurance, which includes a provision for periodic testing, that the most current versions of the source programs and documentation will be held by the escrow agent.

At a minimum, the software documentation held by the escrow agent should include system flowcharts or a system narrative, program source listings, program narratives, file and record layouts, descriptions of individual fields within the records, and calculation routines. Portions of this documentation may be included with the user guides that are provided to the financial institution. These guides also should cover transaction codes and descriptions of input forms and output reports.

Without the source code and the program documentation, program changes are virtually impossible. As long as the financial institution can be assured of access to both, a separate contract programmer may be employed to meet any crises arising from the vendor's failure to provide programming support. Having this recourse substantially reduces the potential risk to the financial institution.

Third-party Programming

The option of hiring a third-party programmer to develop unique software or modify existing software to meet the financial institution's needs is not common, because of the proliferation of existing software packages. Although this option is a viable alternative, serious problems can occur when:

- There is a misunderstanding of the requirements between the programmer and the financial institution.
- There is complete reliance on a single individual for programming support.

An experienced programmer, given enough time and money, can create reliable software packages. However, for a financial institution to control the development process properly, it should determine whether the programmer is qualified to perform the work; establish limits on the amount of money it is willing to spend; make periodic payments only as the work is completed; and establish realistic time frames for completing the work. These conditions should be incorporated into a contract that details the responsibilities of each party. When the programming is completed, it should be thoroughly tested under all conceivable conditions to ensure that output is reliable and that each program performs as anticipated. In addition, the financial institution should ensure that program documentation, user guides, and source programs are properly developed and readily available. The institution should ensure that their fidelity bond coverage also extends to contract programmers.

System Software

Each computer system has a collection of programs and procedures known as system software. The system software includes the operating system, system utilities, and compilers or interpreters. The basic purpose of each component is described as follows:

- Operating system – Master program that controls operation of the computer system. It supervises the execution of programs, allocates storage, and handles input and output devices. Some examples are OS/400, Unix, MS/DOS, OS/2, and Pathworks.

- System utilities – Programs that perform repetitive functions, such as creating, deleting or altering files, and copying files for backup.

- Compilers – Programs that translate source programs that are written in high-level languages, such as COBOL, to object programs that the computer can then execute.

- Interpreters – Programs that function similarly to compilers and are used for translating low-level languages into machine language. Unlike compilers, this process must be done each time a program is executed.

Periodically, updates to the software are released and installed by the financial institution. The financial institution may be supplied with numerous manuals describing the system and its capabilities, but it may need to know little about the system software other than control options for password protection, security codes, access control features, and activity logs. Options available in the system should be properly documented, along with management's decisions about the use of such options.

Appropriate controls should be established for source code, compilers, and data-altering utilities. One obvious way to prevent tampering is to remove compilers and data-altering utilities from the system, but this option is not always possible. Certain systems use these utilities during normal production runs. Other systems do not use compilers, but require that the source code be kept on the system and translated into object code each time a program is executed. Controlling risk in these systems may prove especially difficult. In such cases, an activity log should be automatically generated by the system. The logs should record the execution of application programs, system utilities, compilers, user activity, and should provide the nature of the activity, the date, the time, and where the activity was initiated. The activity log should be generated frequently and reviewed routinely by a supervisor or auditor, who has a complete understanding of the information presented in the log. Unauthorized use of data-altering utilities should be investigated immediately.

Even if a compiler or the source code is not on the system, some vendors provide these items upon request. If a financial institution has these items in its possession, they should be placed under appropriate dual access controls. When these programs are needed, their use should be monitored and documented.

RISK AND CONTROL CONSIDERATIONS

See Chapter 25 for additional information on FFIEC SP-2 and its Appendix: Uniform Interagency Rating System for Data Processing Operations.

SECURITY

Risks

- Software may not be available to provide adequate security for client/server environments.
- Adequate physical security for critical hardware components may be lacking due to the distributed nature of the environment and the slow development of security conscious cultures in the client/server arena.

- Inadvertent or intentional unauthorized end user access to software and data presents greater risk of loss in client/server environments due to a potential dependence on the end user to implement some system functions.

Controls

- Adequate steps should be taken to prevent unauthorized access, use of, or changes to, systems or data.

- Procedures should be implemented to ensure the privacy and confidentiality of information.

- Management must review security reports.

COMPUTER OPERATIONS

Risks

- Disaster recovery and business continuation plans may be incomplete or outdated due to more frequent changes to hardware and software resources.

- Exposure to system failures may be increased due to easier software virus infiltration in a distributed environment.

- Incomplete hardware and software inventories could result in additional exposures in the form of unidentified network operations and/or the lack of adequate insurance coverage.

- Management information systems that rely on client/server systems could become incomplete or inadequate due to the lack of adequate operational controls.

Controls

- Procedures should be adequate to ensure the timely, accurate, and complete processing of information.

- Management should ensure that critical systems and operations are recoverable in the event of a disruption in service.

IMPLEMENTATION AND MAINTENANCE

Risks

- Internal control considerations could be neglected due to the shortened time frames commonly found in the development of client/server systems.

- System failures resulting in weaknesses not identified in pre-implementation testing are more likely to occur than in mainframe environments.

- There are increased risks from unauthorized modification of application programs due to the distributed location of the client and its applications.

- Application development costs may consistently be underestimated if a system development life cycle methodology is not used.

- Failure to re-engineer the work flow in the design phase of the application may limit management's ability to optimize the benefits from this technology.

Controls

- Appropriate procedures, including a system development life cycle methodology, should be included in new and existing client/server systems.

- Audit should have involvement in the SDLC process.

SYSTEM SOFTWARE

Risks

- In this heterogenous environment (i.e., consisting of multiple platforms), there is an increased vulnerability to incompatibilities in installed software versions. Thus modifications may cause inconsistent operating results.

Controls

- Management should ensure that systems are properly tested and approved and that modifications are properly implemented.

- Management should determine that adequate version control procedures are properly implemented.

DATABASE MANAGEMENT SOFTWARE

Risks

- Database integrity may be corrupted by deficiencies in the quality of the implementation and the administration of database management systems.

- Lack of database integrity is of greater concern due to concurrent updates of distributed databases which may not have properly established locking capabilities.

- Unauthorized access to the data could occur as a result of inadequate database administration or improper data ownership.

Controls

- Management should implement controls to ensure the integrity and confidentiality of transactions.

- Management should ensure that systems are properly tested and approved and that modifications are properly implemented.

- Management should determine that adequate version control procedures are properly implemented.

- Management should determine that the database management system has adequate recovery capabilities.

MIDDLEWARE

Risks

- System integrity may be adversely effected because of multiple operating environments attempting to interact concurrently.

- Lack of proper software change procedures across multiple platforms could result in a loss of system integrity.

Controls

- Management should implement controls to ensure the integrity of the client/server networks.

- Management should ensure that systems are properly tested and approved and that modifications are properly implemented.
- Management should determine that adequate version control procedures are properly implemented.

CONCLUSIONS

This section reviewed many of the controls that should be evaluated in financial institutions with end-user computers. In evaluating these systems, auditors and examiners should assess whether the institution's established standards, policies, and procedures are adequate to control the inherent risks that are present in end-user computing environments. In addition, auditors and examiners should determine the degree to which the users adhere to those standards, policies, and procedures.

Acquiring an end-user computer system requires careful planning and the active involvement of senior management. Professional organizations in both data processing and the financial community offer training that provides a nontechnical approach to understanding computers. With this background, senior management can better guide the acquisition and implementation of end-user systems. The failure to understand the capabilities and limitations of automated data processing systems has produced costly and unsatisfactory results for some institutions.

End-user computer systems will continue to proliferate as a relatively low-cost option for meeting the data processing needs of financial institutions. These systems are already valuable tools to support managerial objectives in many financial institutions. The value of these tools is increased by an effective system of controls that ensures the data integrity and security of information processed on these systems.

END-USER COMPUTING WORKPROGRAM

CHAPTER 16WP

(FILE NAME ON DISK # 3 = IS-WP#11.WPD)

COMMENTS

This section is intended to determine the adequacy of controls over the use of micro/mini computers in the institution. The degree of control necessary will depend on the reliance the institution places upon micro/mini computers for significant and/or sensitive processing. The remaining steps will be completed only for those areas in the institution, if any, that rely on micro/mini computers for significant and/or sensitive activities. Document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

Tier I

1. Obtain a list of micro/mini computers and the applications processed on them. The list should indicate:

   a. The number and type of micro/mini computers by functional area.

   b. The applications processed on the micro/mini computers, including the software used and its functions.

   c. The institution's estimate of the importance and sensitivity of the information (indicate high, medium, or low).

POLICY AND STANDARDS

2. Determine the adequacy of the institution's micro/mini computer acquisition policy for both hardware and software and whether:

   a. Centralized control and/or purchasing is used.

   b. There is an approved list that must be adhered to (e.g., system or corporate architectural standards).

3. Determine if the institution has an information center/help desk to support the use of micro/mini computers.

4. Determine if written policies and standards exist, and if all employees are aware of them, including:

   a. Micro/mini computer programming.

      1. System development.

      2. Program change control.

b. Program documentation standards.

c. Restrictions on the use of micro/mini computers and the data they contain and/or generate. This should include a prohibition against the copying/-piracy of software.

d. Security.

5. Determine if any data processed is significant and/or sensitive to the institution. If no significant/sensitive data is being processed, proceed to step 10.

STAND ALONE/LOCAL AREA NETWORKS

6. Determine whether micro/mini computers operated in a LAN or stand alone environment are the primary system for any significant and/or sensitive applications. If so, review controls in line with mainframe processing, using applicable sections of the workprogram (e.g., EDP audit, and systems and programming sections).

MICRO/MINI COMPUTERS LINKED TO MAINFRAMES

7. Determine if the micro/mini computers are and/or can be linked to the mainframe processor by dial-up lines or direct connection. Distinguish between dumb terminal and peer to peer or smart terminals.

TRAINING

8. Determine the level and type of training provided for the use of micro/mini computer hardware and software.

DISASTER RECOVERY/CONTINGENCY PLANNING

9. Determine the level of disaster recovery/contingency planning provided for the micro/mini computers, including:

a. Hardware.

b. Software, especially custom software.

c. Off-site storage and/or recreation of the data files.

CONCLUSIONS

10. Review the results of work performed in this section and in sections for planning, audit, and

management. If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

11. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

12. Assign rating (See Chapter 5 for additional information.)

13. Prepare an index of workpapers for this section of the workprogram.

14. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations .

15. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner	**Date**

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

POLICY AND STANDARDS

1. Determine whether policies, procedures, or standards exist for:

   a. Software and hardware acquisition, including:

      1) Cost benefit analysis.

      2) Approved list.

      3) Programming standards.

      4) Change control.

      5) Documentation standards.

      6) Testing.

      7) Ownership of programs, spreadsheets, etc., developed on the institution's time and equipment.

      8) Limitations on in-house software development.

   b. Micro/mini computer use, including:

      1) Use of the output/data.

      2) Restrictions on personal and nonjob related use.

      3) Use of personal equipment and/or software.

      4) Use of unauthorized software.

      5) Modification of the hardware and or software.

      6) Copying or piracy of the software.

      7) File backup.

      8) Confidentiality of data.

2. Verify whether housekeeping procedures have been developed and enforced to provide protection from:

   a. Food.

b. Liquids.

c. Dust, smoke.

d. Magnetic fields.

3. Determine whether procedures have been developed and enforced for:

   a. Backup and off-site storage of critical information.

   b. Inventory control on the hardware software.

4. Determine whether adequate security measures have been established, covering:

   a. Physical security.

      1) Restricted area.

      2) Key locks on the machines.

      3) Removing and securing the data files.

   b. Access controls.

      1) Passwords.

      2) Encryption of data on the disk.

      3) Use of dial-up equipment.

      4) Read only attributes to the files.

5. Proceed to step 10, Tier I.

Examiner	**Date**

Reviewer's Initials

DOCUMENT IMAGING CHAPTER 17

(FILE NAME ON DISK # 2 = S2C17.WPD)

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 the board of directors who must ensure that the risks are addressed by the institution's management (see Chapter 25 for additional information on FFIEC SP-10.)

DEFINITION

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

Imaging systems capture customer documents and store them in a digital form through the use of scanning devices. Additional data and text may be entered into the system as part of the customer record. The document is imaged, and the data and text are then indexed and stored for later retrieval at user workstations throughout the financial institution. Imaging systems can be designed to range from a small standalone system supporting work groups or departments, to large systems supporting multiple documents with hundreds of users. Images are stored on standalone optical disks, an optical jukebox, or magnetic disk. Peripherals such as scanners and laser printers are managed by LAN-based servers. Thus, the components of imaging are: capture data, store data, display data, print data, and transmit data.

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 lowspeed 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 automatic routing of electronic documents to individuals involved in the review or decision making process. They also can 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 include:

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 scanning document. Procedures should be in place to ensure original documents are not destroyed before it has been determined a good image has been captured.

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 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, including rotating duplicate optical disks off-site.

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.

COMPONENTS OF THE SYSTEM

The components or parts of optical filing systems are:

- Document scanner.
- Personal computer(s) (e.g., 386, 486, Pentium system) capable of running the image software, DOS-based software, and Windows.
- A high resolution, non-glare, large-landscape monitor that allows clear viewing of documents, while offering windows for viewing portions of other documents, creating documents, or running other applications.
- An optical-disk drive that may contain a three and a half, five and a quarter, 12" or 14" for storage. The disks may be write-once or rewritable.
- A "jukebox" that stores and retrieves imaged data.
- A laser printer that provides high-speed printing.
- Local area networks/wide area networks.
- Upgrades of mainframe computers are required for imaging, as well as image-capable check encoders and sorters, for a check processing environment.
- Application software used for text retrievals and searches, and image management.

BENEFITS

Most areas of the institution could benefit from the use of imaging systems. Examples of potential uses are: check/item processing signature verification mortgage loan servicing loan origination and trust file and pension fund management. Some benefits derived from an optical system are:

- Increases productivity.
- Improves service (fewer lost documents).
- Improves the business process/electronic work flow.
- Reduce business costs (e.g., reduced floor space, file cabinets, and labor) since 100 cases of paper are stored on one 5 1/4" optical disk. This would be equal to 750,000 customer statements. A bank can mail two checking account statement pages and two imaged pages (36 checks) to a customer, which weighs one ounce. In a conventional environment, the statement and checks would weigh two ounces.
- Positions for the future.
- Improves control over paper files and reduced

deterioration due to handling.

- Gives access to data by multiple locations.
- Allows simultaneous usage of the same material.
- Increase potential market share.
- Provides opportunity to learn hands-on.
- Reduces fraud, especially credit card fraud. Customers' pictures are stored and their images are transmitted to credit card merchants for purchase verification.
- Enhances employee skill sets.
- Yields higher profits.

RISKS

- Legal issues.
- Longevity of optical disks is unknown (i.e., shelf life claims range from 10 to 100 years).
- Major impact on the way a financial institution operates.
- Developing standards.
- Very costly (including conversion process).
- Maturity of vendor/product.
- Problems with character-recognition process (i.e., for check processing, some software is correctly reading check dollar amounts only about 50 percent of the time). This is due to the quality of the checks.
- Loss of data.
- Images indexed incorrectly.
- Incomplete document set.
- Access to paper documents.
- Fraud – deliberately altering, destroying, or counterfeiting images.
- Hiring and keeping an adequate number of skilled personnel who are knowledgeable about imaging.

Examples of Imaging Testing or Use

The following are examples of how imaging is being used or tested:

- To decipher handwritten dollar amounts on checks.
- To reduce the back-office proof of deposit function.
- To transmit images of checks in return-item notification, and canceled checks that are held or truncated, at the point of deposit.
- At a credit card customer service center, incoming mail is now scanned as soon as correspondence is opened. This permits customer service to know when letters arrive, the actions taken, and when. In addition, customers' account histories are available on-line. As a result, telephone service levels have improved, and the average speed of answer was reduced from 2 minutes to 12 seconds.
- A desktop imaging pilot for 8,000 Lotus Notes users will store, retrieve, print, and fax documents. Imaging is used in new construction projects. Source documents such as invoices, canceled checks, technical specs, building permits, contracts, and purchase orders will all be imaged. Hence, facilities management is becoming image-enabled. All images are linked to the bank accounting system.
- A mortgage processing center is actively using imaging for all mortgage-related documents; IRA/CD were imaged as well as all documents in the retail loan area were imaged.

IMPLEMENTATION

Banks and other corporations are focusing on applications to scan that are manageable, visible, and valuable, so that success will attract the support of top management. As imaging becomes integrated into the mission critical processes of a financial institution, integrity must be maintained, and the adequacy of controls should be ascertained. Image-processing systems are configured similarly to other information services environments with the exception that a new data type (digital image file) has been introduced, and that new capture peripherals (scanners) and storage media (optical disk) are involved.

This section is intended to determine the adequacy of the institution control over its electronic document imaging systems operations. The levels of controls will depend on the degree of reliance the institution places on its imaging operation. Systems could vary from small isolated local scanning/recordkeeping to financial, customer database information files, and highspeed check processing. The imaging system operations should be reviewed in consideration of the importance of the information/data to the institution rather than its size. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

Tier I

MANAGEMENT CONTROLS

1. Evaluate the adequacy of general controls that have a direct effect on the imaging system, such as cost benefit studies, physical security, data security, documentation, error handling, program change procedures, system recoverability, and vital records retention.

2. Evaluate the overall adequacy of controls for the integrity documents scanned through the system (accuracy and completeness). These documents are converted from paper to a machine readable format and must remain in the system during conversion.

3. Ensure that appropriate controls are in place prior to destruction of source documents (e.g., shredded) after being scanned through the imaging system.

4. Ensure that compliance with regulations and standards is being enforced by management.

5. Ensure that the imaged departments or applications have been incorporated into the financial institution's contingency planning procedures.

6. Determine if a segregation of duties is in place, where the imaging occurs. This ensures that the work of one person is reviewed by another, that a specialization of tasks has been created, and that any instances of fraud are inhibited.

TRAINING

7. Determine whether an adequate technical training program exist for users, operators, and staff.

CONCLUSIONS

8. Review the results of work performing in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

9. Discuss with management:

   a. Violations of law, rulings, regulations, or significant internal control deficiencies.

   b. Recommended corrective action for deficiencies cited.

   c. Management's proposed actions for correcting deficiencies.

10. Assign rating (see Chapter 5 for additional information.)

11. Prepare an index of workpapers for this section of the workprogram.

12. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

13. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner	**Date**

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

MANAGEMENT CONTROLS

1. Has an imaging system been installed at the institution? Describe its functions and the responsibilities of the department/staff.

2. If no, explain whether issue is being explored and studied, relative to future bank technologies.

3. If yes, explain whether it complements the financial institution's current technology structure.

4. If yes, explain how the system is/was justified.

5. If installed, obtain dates.

6. Determine whether the stated benefits are obtained.

7. For the imaging project, assess whether management developed a set of clear, manageable and measurable goals, relative to the processing environment, technology choices, and external/internal influences.

8. Review the overall business components of the process:

   a. Strategy.

   b. Application Selection.

   c. Implementation.

   d. Roll-out.

9. Determine whether all pertinent personnel have been involved.

10. Identify the risks that were taken.

11. Determine whether the workflow is installed and operating correctly.

12. Prior to the introduction of imaging, determine whether a pilot team assessed controls, system benefits, etc.

13. Determine which of the following comprises this pilot team:

    a. End Users.

    b. MIS.

    c. Audit.

    d. Data Security.

    e. Bank Operations.

14. Verify whether management contacted any organization to obtain assistance on imaging guidelines. (Note: Examples of such organizations are Association for Information and Image Management; Department of Defense; American Banking Association; the American National Standards Institute; National Automated Clearing House Association; National Association for Check Safekeeping; and the Electronic Check Clearing House).

INFORMATION SERVICES

15. Describe how the Imaging System communicates with the host and whether the host is:

    a. LAN.

    b. T-1.

16. Determine the imaging system's capacity and future growth capability.

17. Describe the topology being used and whether it is:

    a. Mini-based.

    b. PC-based.

    c. Mainframe-based.

18. Identify the vendor and who assessed its reliability. (Note: If Information Services personnel have retained files on the vendor analysis, review this file to determine the justification of selecting a particular vendor).

19. Since companies use different imaging standards, define the imaging standard being used.

20. Describe the migration issues that have been addressed relative to moving to the next generation.

21. Describe how document conversion is being accomplished. Examples include: back-file conversion; as you touch; and only new documents.

22. Determine whether plans exist to share documents between departments and whether branches are using imaging (teller and customer service areas accessing images through desktop computers).

23. Describe the back-up procedures, including:

    a. Dual optical disks.
    b Tape back-up.
    c. Optical disks.
    d. Digital audio tape (DAT).

24. Describe the financial institution's disaster recovery procedures for imaging, including:

    a. Recovery at the institution's own site.
    b. Recovery at the vendor's site.
    c. Another company, completely separate from the bank.

25. Identify which of the following performs the hardware maintenance:

    a. End-user.
    b. Information services.
    c. Vendor.
    d. Other.

26. Identify which of the following performs the programming and on-going programming enhancements:

    a. End-user.
    b. Information services.

c. Vendor.

d. Other.

27. Identify which of the following provided and continues to provide programming documentation:

    a. End-user.

    b. Information services.

    c. Vendor.

    d. Other.

29. Describe whether users understand the technology and have received training on imaging.

30. Determine whether both users and Information Services personnel are satisfied with the quality control of scanned documents.

31. Evaluate whether the financial institution acquired any PC-based systems that analyze the condition of checks (if check processing imaging occurs), prior to the information being imaged.

32. Describe the recovery of bad images by using:

    a. Re-scan ALL.

    b. RE-scan ONLY defective images.

33. Describe the recovery from hard/optical disk by using:

    a. Back-up tape.

    b. Optical copy.

    c. Re-scan all documents.

34. Describe how the indexing of documents is performed. (Note: Proper indexing at the time of capture is critical for retrial and authorizing access levels to documents. The integrity of indexes must be carefully maintained to ensure that electronic documents can be located and accessed quickly and accurately. Poorly designed indexes can result in lost documents).

    a. After each document is scanned.

b. After all documents are scanned.
c. Indexing controls.

35. Determine whether the imaging hardware is interchangeable with other vendors hardware (i.e., imaging hardware is used to display or print the storage).

36. Determine whether the imaging software is interchangeable with other vendors software (i.e., imaging software is used to locate the stored image).

37. Determine whether the financial institution can migrate to the next generation of hardware.

38. Determine whether the financial institution can interchange documents with other vendor systems through such devices as:

    a. Fax.
    b. LANs.
    c. Wide area networks.

39. Describe whether plans exist to share documents between departments.

40. Assess whether management from information technology or top management conferred with the bank's legal department to determine if documents should be destroyed after the Imaging process was completed.

41. Define the retention period for source documents. (Note: The law may vary from state to state).

42. Define the retention period for image documents. (Note: The law may vary from state to state).

43. Evaluate whether the financial institution can prove in court that documents cannot be changed prior to storing on optical disk.

44. Define the audit trail detention period.

45. Determine if vendors who provide imaging service were asked to sign non-disclosure agreements.

SECURITY CONTROLS

46. Obtain an understanding of access security controls. Examples include:

    a. Maintaining a Data Security Administration function.

    b. Maintaining written procedures for information security relative to imaging.

    c. Controls over an electronic imaging file, preventing the manipulation of bytes.

    d. Controls over the image underlying index, preventing the writing over an existing image.

    e. Controls over the index file, preventing this file from being tampered with or damaged. Such damage or destruction would severely hinder the system's ability to locate and retrieve data.

47. Determine if security violation and other pertinent reports are being reviewed and ensure that other controls are in place for: (Note: Mainframe software security, such as RACF or ACF2, can add a level of security on the index data in imaging. Incorporating imaging with adequate access controls requires implementing independent layers of software security).

    a. Password length.

    b. Maximum number of logon attempts, before user ID is suspended.

    c. Mandatory changes of user passwords (e.g., every 30 days).

    d. DES encryption on disk and storage.

    e. Limiting users to authorized applications.

    f. Limiting users to authorized data/records.

    g. Alterations of data by authorized users.

    h. Terminal time out feature for inactivity.

OTHER CONTROLS

48. Determine if controls are in place to prevent the system from booting from other media (e.g., floppy disk) or access any other disks, bypassing security controls.

49. Ascertain if controls exist over such sensitive software as:

    a. Software that can modify images.

    b. Software that can cut and paste.

    c. Software that can alter or bypass security.

50. Determine whether image back-ups are stored away from the primary location of the financial institution and whether they may be performed by making dual optical disk copies.

TRAINING

51. Determine weather policies and procedures are in place to ensure adequate technical training of the users, operators, and staff.

52. Determine whether adequate documentation exists for use in training and as a reference material for all systems and application functions.

53. Assess whether security and control concerns are part of the education and training programs for the users, staff, and operators.

54. Evaluate how corporate policies are communicated to personnel relative to training programs.

55. Assess how changes to the system are accounted for in training and education programs, including documentation and work aids.

56. Proceed to procedure 8, Tier I.

Examiner	**Date**

Reviewer's Initials

WHOLESALE EFTS (ELECTRONIC FUNDS TRANSFER SYSTEMS)

CHAPTER 18

(FILE NAME ON DISK # 2 = S2C18.WPD)

Electronic Funds Transfer Systems (EFTS) have become the primary method employed for large-dollar (wholesale) payments made by financial institutions and their business customers. It also is also an important and expanding element of retail payment systems. EFT is defined as any transfer of funds that is initiated through an electronic terminal, telephonic instrument, computer or magnetic tape to order, instruct, or authorize a financial institution to debit or credit an account. The ability of financial institutions to provide these services is a direct outgrowth of the rapidly improving computer and data communications technology.

EFT covers a wide-range of applications that, while for control purposes must be separate from direct IS activities, are often highly dependent on IS operations. Even systems not directly interfaced with a financial institution's IS operations, such as direct Fedwire and terminal connections with correspondent institutions, transmit data electronically. As a result, examiners familiar with information systems must be involved with the review of EFTS activities, since even non-IS related activities such as credit monitoring, payment authorization, and management reporting depend on systemically reliable and secure automated controls.

For U.S. financial institutions, the bulk of large-dollar payments are made through the Fedwire and CHIPS payments systems. While still primarily used for retail payments, an increasing number of large-dollar payments are made by means of automated clearing houses (see ACH Chapter 21). Other retail funds transfer services (see Chapter 20) include automated teller machines (ATMs), point-of-sale (POS) systems, telephone bill paying, and home banking systems, which are gaining widespread customer use.

Critical to any payments system is the method employed to generate payment instructions. Payments systems are supported by a variety of electronic message networks that deliver payment instructions, including SWIFT, telex, and in-house data transmission terminals. Payment instructions also may be generated by partially electronic or manual sources including telephone, fax, letters, memos, and standing instructions.

In view of the potential for material loss through error, inadequate control, or fraud in EFT systems, it is imperative that financial institutions establish a strong internal control environment over these activities. Furthermore, senior management regularly should be made aware of inherent risks associated with the various systems together with any changes in the environment.

WHOLESALE OR LARGE-DOLLAR FUNDS TRANSFER SYSTEMS

FEDWIRE

Fedwire is the Federal Reserve System's nationwide electronic funds and securities transfer network. Fedwire links the 12 Federal Reserve Banks with a large number of depository institutions that maintain reserve or clearing accounts with the Federal Reserve. On a daily basis, Fedwire processes approximately $1.4 trillion in funds and securities transfers. The Fedwire funds transfer system provides the electronic transfer of immediate and irrevocable payments between participating institutions and functions as both a clearing and settlement facility. The Fedwire book-entry securities transfer system provides for the transfer of U.S. government and federal agency securities that settle on the books of the Federal Reserve. The Fedwire service may be accessed by direct computer interface or off-line by telephone through a PC-based electronic delivery system named Fedline. Fedline was developed by the Reserve Banks and uses dial-up lines for network access. (See Chapter 19 Fedline EFT for additional information.)

The Fedwire fund transfer system is a credit transfer system. Each funds transfer is settled individually on the books of the Federal Reserve as it is processed, and is considered a final and irrevocable payment. A depository institution that sends a funds transfer irrevocably authorizes its Reserve Bank to debit (charge) its account for the transfer amount, and further authorizes the Reserve Bank of the receiving institution to give credit in the same amount to the payee. The Federal Reserve guarantees immediate availability of funds; once the Federal Reserve bank credits the receiving institution's account or delivers the advice of payment, the Federal Reserve Bank will not reverse credit for the payment. Therefore, there is no settlement risk to the recipient of a Fedwire Transfer. The Federal Reserve Bank assumes the risk if the sending bank overdraws its position at the Reserve Bank. The Federal Reserve's payments system risk policies are specifically designed to limit the risk that a sending bank fails with its reserve account overdrawn. Reserve Banks require that depository institutions continuously monitor and adjust their reserve account positions to ensure adequate funds are on hand, or that they are in compliance with established overdraft limits and collateral requirements. Other risks associated with Fedwire funds transfers include potential loss due to errors, omissions, and fraud.

CHIPS

The Clearing House Interbank Payment System (CHIPS) is a funds transfer network owned and operated by the New York Clearing House Association (NYCHA) to deliver and receive U.S. dollar payments between banks, domestic and foreign, that have offices located in New York City. The network is composed of a small number of settling participants (large U.S. chartered banks that settle end-of-day balances between each other) and a larger number of non-settling participants who maintain accounts with one of the settling banks. Settling participants settle for non-settling participants. The majority of CHIPS payments are for settlement of U.S. dollar foreign exchange contracts and Eurodollar investments.

CHIPS is a multilateral net settlement payments system. Unlike Fedwire funds transfers, CHIPS transfers are not settled at the time the payment instructions are delivered, but instead are settled at the end of the day through a net settlement arrangement established with the Federal Reserve Bank of New York. The Federal Reserve Bank of New York provides CHIPS with a special settlement account that is open to the settling participants only during the settlement period. Based on a net settlement report prepared by CHIPS at the end of each business day, CHIPS participants in a net debit position remit payments via Fedwire to the special account and, after all debit payments are received, the banks in a net credit position are paid.

Payment messages over the CHIPS network are irrevocable obligations of the participant. NYCHA has established rules that address the possibility of a participant failing to settle. Under these loss-sharing rules, all other participants are obligated to pay a share of the net debit balance of the failed participant. The rules are based on a defined formula that initially includes a pro-rata apportionment based on a participant's activity with the failed participant. This additional settlement obligation is collateralized in advance.

In order to limit the risk created by an individual participant, CHIPS adopted bilateral credit limits and net debit caps related to intraday net debit positions. Bilateral credit limits establish a limit on the net value of payments each participant is willing to receive from each of the other participants. The limit may be as high as 20 times the amount of collateral that the participant holds with CHIPS and may be revised on an intraday basis. The CHIPS system automatically rejects any payment in excess of the bilateral limit. Net debit caps are a function of the bilateral credit limits extended to a participant by all other participants and represent the maximum permissible debit position by a participant during the day. The net debit cap is 5 percent of the sum of all bilateral credit limits extended to a participant by other CHIPS participants and is set each morning. Payments that exceed the cap will be rejected.

CHIPS is not responsible for losses resulting from system errors. Such losses are settled by the participants. If a participant commits a fraud, that participant will bear the loss. CHIPS maintains

insurance coverage for possible fraud losses committed by employees. Losses exceeding CHIPS insurance coverage are shared on a pro rata basis of each participant's dollar amount of transfers for the preceding month.

Other Related Systems

Indispensable components of funds transfer activities are the message systems employed by customers to originate payment orders, either for their own benefit or payment to a third party. Unlike payments systems, message systems process instructions to move funds and administrative messages. The actual funds movement is accomplished by debiting the originating customer's account and crediting the beneficiary's account. If the beneficiary's account or the beneficiary bank's account also are with the originator's bank, the transaction is normally handled internally via book-entry. If the beneficiary related accounts are outside the originating customer's bank, the transfer may be completed by use of a payments system, such as Fedwire or CHIPS. The means of arranging payment orders range from manual methods (e.g., memos, letters, telephone, fax, or standing instruction) to telecommunications networks. These networks may include those operated by the private sector, such as SWIFT or telex, or operated internally by or for the institution. The internal networks can be for intercompany purposes only or connected to both intercompany and customer sites.

Since the payment order is the institution's authorization to act on behalf of the customer it is imperative that a system is in place to establish the authenticity and time of receipt of the order. These two elements are the primary components cited by the Uniform Commercial Code Article 4A (UCC4A) in establishing responsibility for the execution of a payment order. UCC4A, which has been adopted by a majority of the states in the United States and incorporated into the Federal Reserve System's Regulation J, establishes liability for improper or untimely processing of a payment order, or cancellation, from initiation to final execution of the originator's instructions. Included in UCC4A is a requirement that a security agreement acceptable to both the financial institution and the customers be established

Several phases exist in funds transfer operations where inappropriate or incorrect use of the system can occur. As a result, there is a need for a clearly defined authentication procedure throughout the process. Effective controls should be established over the following areas:

- The original instructions from the customer to the financial institution (e.g., account officer, branch manager, and terminal entry).
- Every transfer point of data for each step of the manual process (e.g., account officer, message receipt, authentication, data entry, and payment release).
- Every transfer point of data for each step of an automated process (e.g., SWIFT/telex, message preparation, data entry, and payment release).

The following is a summary of various message systems:

- *SWIFT* – Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a nonprofit cooperative of member banks serving as a worldwide interbank telecommunications network, based in Brussels, Belgium. SWIFT operates three fully redundant operating centers in Brussels; Amsterdam, Netherlands; and Culpepper, VA, that can function in a standalone mode. Unlike EFT systems, SWIFT only provides instructions to move funds. SWIFT does not have a settlement mechanism. The actual funds movement is accomplished via debits and credits to correspondent accounts maintained at participating institutions. SWIFT messages may be used to transmit instructions either domestically or internationally. Many high volume funds transfer institutions interface SWIFT directly with their automated payments system. As a result, entries pass through the system without human intervention unless programmed conditions (e.g., overdraft limit excesses) or message errors occur. SWIFT provides transaction reports necessary for system reconcilement. The SWIFT system employs dual passwords for data entry and release of certain messages (e.g., funds payment orders). Once properly

entered at the point of origination, the SWIFT network controls the integrity of the messages, thus there is no requirement for the receiver to reverify payment orders.

- *Telex* – Several private telecommunications companies offer worldwide or interconnected services that provide a printed record of each message transmitted. Telex is the primary message system for institutions that do not have access to SWIFT. Access to Telex systems can be by dial-up or dedicated line connections through teleprinters. Some systems are monitored by computer around the clock, seven days a week and are fully redundant with automatic switch over and recovery capability. The companies which process the majority of volume include Western Union, RCA Globe, ITT World Communications, and Money Gram. The Telex systems do not include built-in security features. Users of Telex exchange security codes and senders numerically number messages sent to another given institution. It is the responsibility of the sending institution to incorporate a test key in all instructions to a receiver to execute a payment order. The receiver is responsible for the safekeeping of the unique test code keys of each sender and the decoding of each test message. This function must be clearly separated from the Telex operating area and funds payment function. Due to the lack of uniformity and the uniqueness of the various test codes, only a few institutions employ fully automated interface of Telex with their funds payments systems. However, such interfaces are increasing.

- *In-house Terminals* – Several institutions employ terminals, connected via telecommunications networks with customers' and the institution's operating departments, to execute funds payment orders. These systems may be dial-up or dedicated lines and are often fully interfaced to the institution's funds payments system. The primary security method is the use of unique passwords for each user of the system. Since there is often no intervention by the funds payment operation, it is necessary to establish controls directly in the area employing the terminals. These controls should cover origination, data entry, and release, and should be the same as those associated with an independent funds payment function.

- *Non-automated Payment Order Origination* – While the aforementioned systems are the primary sources for payment order origination, smaller institutions, and some operations in larger institutions (e.g., private banking) still rely heavily on memos, letters, telephone, fax, or standing instructions. (Note: standing instructions are normally maintained in the automated funds transfer system as recurring transfers and should be subject to the same input/verification controls as wires when first entered into the system.) It is imperative that an institution utilizing these payment order methods have a viable security program, including:

  - Signature lists to be maintained and used for internally and externally generated memos, letters or fax instructions. As noted in UCC4A Section 201, signature verification alone is not defined as a security procedure; however, it may be used with other security devices such as call backs or codes.

  - Call back to authorized individuals for both internally and externally generated telephone instructions; and

  - Procedures covering standing instructions protecting against unauthorized change, periodic review to validate accuracy, and ensuring execution under the agreed terms.

CONTROLLING PAYMENT TRANSFER RISKS

Depository institutions, their primary regulators, and the Federal Reserve have been focusing increased attention on the credit risks inherent in large-dollar funds transfer systems. Credit risk is the risk that a party to a funds transfer will fail to settle for the transfer. This risk arises when a financial institution or a Federal Reserve Bank executes a payment order before it has received covering payment from its customer, i.e., when the transfer results in a daylight overdraft in the account of the sending customer. Many depository institutions incur intraday, or daylight, overdrafts in their accounts held at the Federal Reserve as a result of Fedwire funds transfers sent and book-entry

securities received against payment. Similarly, institutions often permit their corporate customers to incur intraday overdrafts.

In principle, an institution engaging in this practice is extending credit to its customer. In most cases, the overdraft is eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day. Since daylight overdrafts constitute an extension of credit – no matter the period of time involved – institutions' credit policies should include provisions for approving and monitoring intraday credit lines to customers.

Intraday overdrafts also may result in disruption of the settlement process for private large-dollar wire transfer systems (e.g., CHIPS). In fact, the failure of one participant to settle on a given day could create settlement problems for other participants who may be relying on credits from the failed institution to settle their own position. As noted above, CHIPS has instituted several controls to alleviate this potentiality, including bilateral credit limits, net debit caps, and collateralization.

The Board of Governors of the Federal Reserve System's payment system risk reduction program (FRRS 9-1005) is designed to control and reduce the intraday credit risks to depository institutions and the Federal Reserve. The policy establishes intraday payments system cap procedures based on a financial institution's own self-assessment and defines the role that the Federal Reserve and other financial institution supervisors will perform in monitoring, examining and counseling depository institutions regarding these matters.

EXAMINATION CONCERNS

There are three primary wholesale EFT examination objectives:

- To minimize systemic risk from payment activities.
- To identify weaknesses in payments operations that could jeopardize the condition of the bank.
- To assure that proper records are available to assist law enforcement authorities pursuing illegal payments activities.

Examiners should be aware of the various levels of risk in funds transfer operations, the potential effect of such risk on the examined institution, and the associated regulatory policies established to control these risks. Funds transfer examination procedures should include evaluations of credit risks, operational controls, communications controls, and audit activities. Also refer to the *Guide to the Federal Reserve's Payments System Risk Policy* for additional guidance.

Evaluation of Credit Risks

Financial institutions should be able to monitor and control their overall position across all payment systems in which they participate. Institutions also should monitor the position of individual customers and control the amount of intraday credit extended to each customer within approved credit limits. Guidelines should be established regarding payments that may exceed approved intraday and overnight overdraft limits, including the consideration that is given to projected incoming payments.

The examination procedures applied to these credit exposures should include:

- Review of established customer credit limits and of the frequency and scope of internal credit reviews. In the absence of preauthorized limits, examiners should determine the process for management approval of daylight overdrafts. Authorization should be within the lending authority of approving officers.
- Review of reporting and approval procedures for payments exceeding established credit limits to ensure that approvals are made by officers with sufficient lending authority.
- Review of intraday overdrafts incurred for compliance with established limits, approval and reporting requirements.
- Review of arrangements/agreements regarding collateralization of credit exposures.

Overnight overdrafts should be reviewed as part of the appraisal of the examined institution's loan portfolio. The examination procedures applied to these transactions should include:

- Analysis of credit worthiness of all borrowers with amounts outstanding in excess of the credit line selected for the overall examination. The credit evaluation procedures should be the same as those applied to any other form of short-term credit.

- Review of reporting and approval procedures for overdrafts and settlement credits exceeding established limits.

- Assessment of reporting and approval procedures for payments against uncollected funds.

Private Netting System

The Federal Reserve has instituted minimum risk management standards for private multilateral large-dollar payments networks and their participants (FRR 9-1021). In order to satisfy these standards, the Federal Reserve expects that individual large-dollar multinational netting systems will utilize the following risk management measures, or their equivalent:

- Each participant must establish bilateral net credit limits – the maximum value of transfers it is willing to receive in excess of the value sent on that network.

- Net debit caps should be established for each participant in the network and monitored in real time.

- The network must develop and implement a system that would not allow the participant to breach either its bilateral net credit limit or sender net debit cap.

- The network must establish liquidity resources, such as cash or collateral, at least equal to the largest single net position.

- The network must establish rules and procedures for the sharing of credit losses among network participants.

Evaluation of Operational and Communications Controls

The evaluation of an institution's operational controls relating to funds transfer activities should be coordinated with the overall examination efforts for the institution to avoid duplication of effort. For example, separate funds transfer and payment systems risk reviews are performed, outside the IS examination, in some institutions. The objective of such reviews is to determine that the internal controls in these areas are effective in minimizing the possibility of fraudulent transfers and losses due to errors and omissions resulting from a poor operating environment. The following sections discuss recommended operational and communications controls for funds transfer activities.

Operational Controls

Basic internal control routines must be in effect for any funds transfer operation to ensure that overall integrity is maintained. However, depending on the size of operations, certain steps may not be applicable for some institutions. The Board of Governors of the Federal Reserve System has issued a *Funds Transfer Activities Uniform Examination Procedures Manual* that includes an Internal Control Questionnaire. In addition, the Bank Administration Institute (BAI) published *Process and Control Guidelines for Wholesale Funds Transfer Systems*, which provides control guidelines. The BAI publication divides the scope of funds transfer operations into three general categories: outgoing transactions, transfer system processing, and incoming credit transactions.

Outgoing Transaction Guidelines:

Recommended control objectives for a wholesale funds transfer system:

- Ensure that an outgoing instruction is recorded accurately and that the original instruction is protected from loss or alteration.

- Authenticate the identity and authority of the sender and ensure the accuracy and completeness of the outgoing instruction.

- Ensure that collected balances are available and that they are held for the outgoing instruction. Any deviations must be considered a credit decision.

- Ensure that the original unaltered outgoing instruction is entered into the internal accounting

].

- Maintaining a physically secure environment.
- Implementation of a comprehensive disaster recovery program.
- Standards for developing or purchasing funds transfer systems software and hardware acquisition.
- Personnel hiring and dismissal policies.
- Organizational reporting controls.
- Audit reviews of funds transfer activities.
- Provisions for maintaining compliance with regulatory reporting and review procedures.

Communications Controls

Telecommunications systems employed for EFT can range from a simple connection between the institution and payments system (e.g., Fedline) to terminal connections with customers that pass through the institution's funds transfer system directly to the payments systems. A data security program must be in place that covers each interface and storage point of the system. These may consist of personal identification numbers, passwords or other identifying keys. Also, it may include account numbers, balances, and financial data relating to transactions.

Financial institutions should use encryption as a means of protecting data throughout the EFT system. Encrypting data during transmission allows the institution to scramble the contents of message/payment orders during transmission and limit the value of that information to an interloper even if a transmission is successfully intercepted. Nevertheless, financial institutions should exercise control over data processing personnel who have access to communications equipment and can monitor and record data flowing in clear text from encryption devices.

Disaster Recovery

In view of the criticality of funds transfer operations for the financial institution, its customers and the related financial community, it is imperative that continuity of operations be maintained. A comprehensive and tested disaster recovery plan must be in effect for each financial institution covering all phases of the operation including:

- Computer equipment.
- Message systems (e.g., SWIFT, telex, telephones, terminals etc.).
- Data entry/receipt terminals (e.g., internal, customers, funds transfer networks, etc.).
- Communications equipment (e.g., terminals, telephone, etc.).
- Communications lines.
- Personnel.
- Physical plant.
- Supplies.
- Transportation.

Backup of EFT Systems

In the event that a financial institution's primary system becomes inoperable, the financial institution should have backup procedures commensurate to the significance and volume of the system. The procedures should cover temporary and long-term conditions as well as conditions related to the network and in-house operations. While reestablishing communications is an important factor, immediate concerns should center on the recovery and settlement of transactions in process and ensuring that security and confidentiality of customer data, PINs, account numbers, and balances are not breached. EFT systems backup should be included in financial institutions' overall emergency procedures and disaster recovery plans. Backup plans should be periodically evaluated and tested for adequacy and feasibility.

Insurance

Although computer related employee defalcations are normally covered, financial institution blanket

bond policies normally exclude certain types of electronic funds transfer activities from standard coverage. Separate coverage for ATM, POS and other EFT systems are available and should be suggested to management, particularly if potential risk exposure exists. A decision to self insure an EFT network should be made by the board of directors only after a briefing on the level of exposure. Coverage that can be obtained through riders include:

- Electronic Data Processor Coverage – This is an optional coverage that extends the definition of employee to include outside data processors of personnel.

- Electronic Funds Transfer Coverage – This optional rider covers fraud losses assumed as the result of the debiting or crediting a customer's account based on any electronic instructions, including an EFT system, originating from:

  - Another financial institution.
  - An automated clearing house.
  - Fedwire.
  - CHIPS.
  - SWIFT.

This rider contains a clarifying clause that excludes voice communication by telephone.

- ATM and POS Coverage – The use of ATMs also may require the attachment of a restrictive rider which may exclude any loss due to the unauthorized use of access cards. Each ATM location must be covered by specific amounts of insurance. Regarding POS transactions, many fidelity bonds, covering retailers, have similar exclusions for EFT which will, in effect, leave the store clerks unbonded. However, specialized EFT insurance providing coverage for ATM and POS systems is available. Coverage may be extended to include impostor terminals and errors and omissions through telephone bill paying and automatic transfers.

Audit Activities

An evaluation of the institution's audit function must be performed to determine whether audit activities related to funds transfer operations are comprehensive and effective. Examiners also should review the auditor's opinion of the adequacy of accounting records and internal controls for funds transfer operations. The review of audit should focus on:

- The scope and frequency of the internal audit program with regard to funds transfer activities.

- The adequacy of the audit program in relation to the Examination Work Program.

- Audit reports to determine any control/operating problems disclosed since the previous examination and what corrective measures were taken by management.

- Audit workpapers to ensure that they document adherence to prescribed audit procedures.

- IS audit coverage of new system enhancements and development projects.

- External audit findings and recommendations.

Regulations Governing EFT Transactions

The Electronic Funds Transfer (EFT) Act is the primary federal law governing consumer rights in an EFT transaction involving a consumer asset account. This law requires that the consumer be provided an initial disclosure statement, a periodic disclosure statement, and terminal receipts for all EFT transactions. It also provides for consumer protection for preauthorized debits or credits to an account. It imposes limits on consumer liability for unauthorized transactions and restricts the ability of financial institutions to issue unsolicited EFT access devices (plastic cards). A consumer's right to have the financial institution investigate and resolve billing errors and limitations on the compulsory use of EFT systems also are included in the EFT act. Regulation E, issued by the Federal Reserve, implements the EFT Act.

Section 205.3 of the EFT Act excludes certain transfers from its coverage, including:

- Transfers made through wholesale wire transfer systems, such as Fedwire and CHIPS.

- Securities transfers.

- Certain automatic transfers between a consumer's accounts at the same institution.

- Telephone transfers not made pursuant to a written agreement.

Also, many states have statutes regulating EFT transactions, which are generally patterned after federal legislation. State EFT laws are not preempted except to the extent that they are inconsistent with federal law. However, they are not preempted if they provide more protection than the federal statute.

As previously noted, rules for wholesale wire transfers regarding the rights, obligations, and liabilities of the parties to funds transfers are established by UCC4A and Fedwire funds transfers are governed by the Federal Reserve's Regulation J, Subpart B, which incorporates the provisions of UCC4A. Fedwire book-entry securities transfers are governed principally by federal regulations promulgated by the Department of the Treasury and the various agencies whose securities are held on the books of the Federal Reserve Banks. In addition, most states have adopted the revised Uniform Commercial Code Article 8, which addresses securities safekeeping and transfer arrangements that do not directly involve the Federal Reserve Banks.

MONEY LAUNDERING AND WIRE TRANSFER ISSUES

As financial institutions, law enforcement agencies, and financial regulators have increased their scrutiny of cash transactions, money launderers have become more sophisticated in using all services and tools available to launder cash and move funds, including the wire transfer systems. This section will provide some background and information on how the different wire transfer systems are used by money launderers, and what IS examiners should consider when reviewing a financial institution's wire transfers operations with regard to the Bank Secrecy Act (BSA). In all cases where an overview by an IS examiner surfaces BSA or Office of Foreign Asset Controls (OFAC) related concerns a reference should be made back through the EIC or the area BSA subject matter expert for additional support.

While there are many ways for money launderers to use the wire system, the objective for most money launderers is to aggregate funds from different accounts and move those funds through accounts at different banks until the origins of the funds cannot be traced. Most often this involves moving the funds out of the country, through a bank account in a country with strict bank secrecy laws, and possibly back into the United States. Money laundering schemes uncovered by law enforcement agencies show that money launderers use the wire system to aggregate funds from multiple accounts at the same bank, wire those funds to accounts held at other U.S. banks, consolidate funds from these larger accounts, and ultimately wire the funds to offshore accounts.

Unlike cash transactions, which are more closely monitored, Fedwire transactions and banks' wire rooms are designed to quickly process approved transactions. Wire room personnel usually have no knowledge of the customer or the purpose of the transaction. Therefore, once cash has been deposited into the banking system, money launderers use the wire system because it is more likely that the transactions can be processed with little or no scrutiny.

BSA RECORDKEEPING FOR FUNDS TRANSFER ACTIVITIES

Recent changes to the Financial Recordkeeping and Reporting of Currency and Foreign Transactions – 31 CFR 103, specifies certain reporting and recordkeeping requirements for wire transactions of $3,000 or more.

In addition to these regulatory changes, the Federal Financial Institutions Examination Council issued a policy statement addressing the use of large-value funds transfer for money laundering. The revised regulation and the FFIEC encourages financial institutions to support law enforcement efforts in this area by including, to the extent practical, complete originator and beneficiary information when sending payment orders, including those sent through Fedwire, CHIPS and SWIFT.

These amendments to 31 CFR 103 require each financial institution involved in wire transfer

activity to collect and maintain certain information on the payment order for five years. This additional information includes the name, address, and account number of the originator, and the name, address, and account number of the beneficiary where practical. If the originator or beneficiary are not customers of the institutions, the banks shall attempt to verify the identification information.

WIRE TRANSFER CONTROL CONCERNS

The following list of wire transfer related activities/transactions in a financial institution warrants further attention by management. The appearance of a transaction with these characteristics or features on the list does not mean that it necessarily involves illicit activity, only that it requires closer scrutiny. Many, if not most, listed transactions may be found upon closer inspection to reflect legitimate business activity. However, a financial institution must know its customer to make an informed decision as to the suspicious nature of a transaction. Also a transaction may be suspicious for reasons other than those previously listed.

- Sending and receiving wire transfers (to/from bank secrecy haven countries), without an apparent business reason or when they are inconsistent with the customer's business or history.

- Periodic wire transfers from a personal account(s) to bank secrecy haven countries.

- Frequent or large volume of wire transfers to and from offshore institutions (banking centers).

- Deposits of funds into several accounts, usually in amounts below a specified threshold, and then consolidated into one master account and transferred outside of the country.

- Large volume of deposits to several different accounts with frequent transfer of major portions of the balances to a single account at the same or another institution.

- Instructions to a financial institution to wire transfer funds abroad and to expect an incoming wire transfer of funds (in an equal amount) from other sources.

- Regular deposits or withdrawals of large amounts of cash, using wire transfers to, from, or through countries that are either known sources of narcotics or whose bank secrecy laws enable money laundering.

- Cash/funds or proceeds of a cash deposit wire transferred to another country without changing the form of currency.

- Many small incoming wire transfers of funds received or deposits made using checks and money orders, and all but a token amount almost immediately wire transferred to another city or country, in a manner inconsistent with the customer's business or history.

- Wire transfers received and monetary instruments purchased immediately for payment to another party.

The internal policies developed by management should address *all* business units of the financial institution including: teller and currency operations, sale of monetary instruments, wire transfers, private and correspondent banking, and the fiduciary, loan, international, credit card, and discount brokerage departments, as appropriate.

WIRE TRANSFER MESSAGE

A wire transfer message contains, by design, a minimal amount of information. As discussed in more detail below, Fedwire messages must contain primary information consisting of the sender's and receiver's name and ABA routing number, the amount of the transfer, a reference number, and certain other control information. These messages may contain certain supplementary information, such as the name of the originating party, the name of the beneficiary, the beneficiary's account number, a reference message for the beneficiary, and other related information.

For purposes of an examination, it is important to be able to identify certain information on the message. The supplementary information is identified using three letter codes. These codes

are identified below, but not all information will appear in all messages. In some messages, there may not be any supplementary information at all.

Product Codes These codes identify the type of transfer and are followed by a slash.

- BTR/ *Bank* Transfer, the beneficiary is a bank.
- CTR/ *Customer Transfer*, the beneficiary is a non-bank.
- DEP/ *Deposit to Sender's Account.*
- DRW/ *Drawdown*
- FFR/ *Fed Funds Returned*
- FFS/ *Fed Funds Sold*

Field Tags These codes identify certain supplementary information about the transfer and consist of three letters followed by an equals sign.

- ORG= *Originator*, initiator of the transfer.
- OGB= *Originator's Bank*, bank acting for the originator of the transfer.
- IBK= *Intermediary Bank*, the institution(s) between the receiving institution and the beneficiary's institution through which the transfer must pass, if specified by the sending institution.
- BBK= *Beneficiary's Bank*, the bank acting as financial agent for the beneficiary of the transfer.
- BNF= *Beneficiary*, the ultimate party to be credited or paid as a result of a transfer.
- RFB= *Reference for the Beneficiary*, reference information enabling the beneficiary to identify the transfer.
- OBI= *Originator to Beneficiary Information*, information to be conveyed from the originator to the beneficiary.
- BBI= *Bank to Bank Information*, miscellaneous information pertaining to the transfer.
- INS= *Instructing Bank*, the institution that instructs the sender to execute the transaction.

Identifier Codes Two letter codes preceded by a slash and followed by a hyphen used to identify or designate a number important to the transfer.

- /AC– Account number.
- /BC– Bank identifier code
- /CH– CHIPS universal identifier.
- /CP– CHIPS participant identifier.
- /FW– Federal Reserve routing number.
- /SA– SWIFT address.

Advice Method Codes Three letter codes preceded by a slash used to identify the method of advising the beneficiary of transfer.

- /PHN Advise by telephone.
- /LTR Advise by letter.
- /WRE Advise by wire.
- /TLX Advise by telex.+

The following sample message illustrates the format of a Fedwire message and the use of the above codes:

Mode	**Status**	**Mdc**
PRODUCTION	FT	INCOMING

Error-Intercept	**Rcvr**	**Type**
MSG	123456789	1040

Sndr	**Ref #**	**Amt**
987654321	40922	$1,000,000.00

Sample message text block

ANYBANK NYC/ORG=J.DOE, OSLO OGB=BANK OF NORWAY, OSLO AMER NB SF/CTR/IBK=AMER NB LOS ANGELES BBK=BK OF SOUTH CA, MARIETTA, CA BNF=A.B.INDUSTRIES/AC-89-34567/PHN/(415)555-5555 RFB=INV0123 OBI=EQUIP PURCH

Imad
DATE A1B2345C 678 DATE 1234 DEF5

Omad
DATEGH67890I 1234 5679012

This Fedwire message shows a transfer from Anybank New York City, to American National Bank, San Francisco, for $1,000,000.00. Under the *Rcvr* reading is American's routing number. The transfer was originated by J. Doe in Oslo through his bank (the originating bank), the Bank of Norway, Oslo. Bank of Norway sent the funds

to Anybank, which in turn sent the funds to American National Bank. The funds will be sent to the intermediary bank, American National Bank's Los Angeles bank for credit to the bank of the beneficiary, Bank of Southern California, Marietta, CA. The beneficiary of the transfer is A. B. Industries, and the message contains instructions to credit the amount to A. B. Industries' account and advise the company by phone of receipt of the transfer. Mr. Doe sends information that the wire is for payment of invoice number 0123, which was for the purchase of equipment. The *Imad* and *Omad* numbers at the bottom of the message are added by the Fed and identify the date, time, and receiving and sending terminal. For purposes of examining for money laundering, most of the important information will be contained in the supplementary portion of the message with the field tags. Bank personnel can help decipher messages.

INTERNATIONAL ENFORCEMENT

On December 8, 1992, the Federal Financial Institutions Examination Council (FFIEC) issued the following interagency policy statement to address the problem of the use of large-value international funds transfers for money laundering. The law enforcement community both within the United States and abroad has a growing interest in money laundering through funds transfer systems. The FFIEC supports law enforcement's efforts to identify and prosecute money laundering activities involving large-value funds transfer systems. The FFIEC encourages financial institutions to support law enforcement efforts in this area by including, to the extent practical, complete originator and beneficiary information when sending payment orders, including payment orders sent through Fedwire, CHIPS, and SWIFT.

FATF Background

The President of the United States has joined with the leaders of other nations to sponsor a Financial Action Task Force (FATF).[1] The FATF is primarily charged with developing international guidelines to facilitate the identification and prosecution of money laundering activities.

Historically, law enforcement efforts to curtail money laundering activities have focused on the identification and documentation of currency-based transactions; however, recent investigations have focused on the use of funds transfer systems. The FATF has developed recommendations to provide more complete information about the parties to a funds transfer. This information is useful for law enforcement investigations.

FATF Recommendations

The FATF recommends that the text of every payment order include: the name, address, and account number of the person who initiated the first payment order in the funds transfer (the originator); the beneficiary's name and address, and when possible, account number also should be provided in the message text. The FATF also recommends that the identity of the first bank that accepts a payment order from a nonbank should be noted and retained through all subsequent processing of the funds transfer. (The FATF recognizes that the originator and beneficiary information specified in its recommendations may not be provided in transfers originated in some countries because of provisions contained in local laws.)

In this context, SWIFT and CHIPS have recently issued statements encouraging their participants to include the information specified by the FATF recommendations in funds transfers processed through those systems. The Bank of England has also encouraged financial institutions in the United Kingdom to provide complete originator and beneficiary information when using national, international, and proprietary message transfer systems.

To the extent practical, the council encourages all domestic banking offices to implement the FATF recommendations when sending a payment order over any funds transfer system, including Fedwire, CHIPS, SWIFT, and any proprietary networks.

[1] The FATF was formed as a direct initiative by the heads of state of governments of seven major industrialized countries and the President of the European Communities during an economic summit in July 1989. The total membership of FATF now stands at 28 countries, with the primary representation being law enforcement.

With respect to Fedwire, the council recognizes that the Fedwire format limits the amount of information that can be included in a Fedwire funds transfer. While the Federal Reserve System is exploring changes to the Fedwire format, those changes would require time to implement. In the interim, the FFIEC encourages originating banks to ensure that the nonbank originator, beneficiary, and any instructing bank information is included in each Fedwire funds transfer to the extent possible given the limited size of the Fedwire format and the need to give priority to information necessary for payment processing.

Information concerning the originator and beneficiary may be recorded in the payment order text. For example, if an originator requests depository bank A to transfer funds over Fedwire to a beneficiary of depository bank B, and either the originator or beneficiary information is exceeds the space fields specified for originator or beneficiary information.

When a payment order is received by a bank through one funds transfer system and then executed through another funds transfer system; to the extent practical, information on the originator of the payment order received by the intermediary bank should be included in the payment order sent by the intermediary bank. For example, when a SWIFT message is received by an intermediary bank and subsequently sent to the beneficiary's bank via Fedwire, the originator information on the SWIFT message should be carried forward as space permits to the Fedwire message. If the originator information is lengthy and exceeds the space available in the specified fields, to the extent practical, the remaining information may be included in the message text in optional fields that otherwise will not be used for that payment order.

THE OFFICE OF FOREIGN ASSETS CONTROLS (OFAC)

Another area of consideration which the examiner should address during the review of a wholesale EFT area relates to the Office of Foreign Assets Control (OFAC). This is an agency of Treasury that administers a series of laws that impose economic sanctions against targeted hostile foreign countries to further U.S. foreign policy and national security objectives. The economic sanctions programs of the U.S. government are powerful foreign policy tools. Their success requires active participation and support of every financial institution. The use of economic sanctions goes back to the earliest days of the Republic through trade embargoes, blocked assets controls, travel bans, and other commercial and financial restrictions. There has recently been a dramatic increase in the use of such sanctions on a multinational level through such organizations as the United Nations and the Organization of American States. Management of sanctions on the U.S. side is entrusted to the Secretary of the Treasury.

The U.S. Government mandates that all banks located in the U.S., overseas branches of U.S. banks, and, in certain instances, overseas subsidiaries of U.S. banks, comply with economic sanctions and embargo programs administered under regulations issued by OFAC. In general, such regulations:

- Block accounts and other assets of countries identified as being a threat to national security by the President of the United States (this always involves accounts and assets of the sanctioned countries' governments; it may also involve nationals of the sanctioned countries).

- Prohibit unlicensed trade and financial transactions with such countries. U.S. law requires that assets and accounts be blocked when such property is located in the U.S., is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. The definition of assets and property is very broad and covers direct, indirect, present, future, and contingent interests. Certain individuals and entities located around the world that are acting on behalf of sanctioned country governments have been identified by the U.S. Treasury and must be treated as if they are part of the sanctioned governments.

U.S. banks must block funds transfers that:

- Are remitted by or on behalf of a blocked individual or entity.

- Are remitted to or through a blocked entity.

- Are remitted in connection with a transaction in which a blocked individual or entity has an interest.

If a U.S. bank receives instructions to make a payment that falls into one of these categories, it is required to execute the payment order and place the funds into a blocked account. A payment order cannot be canceled or amended after the U.S. bank has received it. Once assets or funds are blocked, they may be released only by specific authorization from the U.S. Treasury.

This is not intended to be a comprehensive discussion of the sanctions programs. In all cases where a non- compliance examiner is revewing the Wholesale EFT activities of an institution and issues relating to OFAC compliance are discovered contact should be made with the EIC or the agency's Compliance area to determine whether subject matter expert support is necessary. For a complete discussion of legal requirements, consult 31 CFR Part 500 et seq. Users requiring further information or seeking a Treasury authorization should contact the: Office of Foreign Assets Control, Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Washington, D.C. 20220. Phone: (202) 622-2490, or 1-800-540-6322. Fax: (202) 622-1657.

The objective of this section is to determine the adequacy of controls over an EFT environment. Although these applications should be operating outside of the IS environment, they depend highly on computer operations. The procedures are set up so that they may be implemented separately as part of either the IS or safety and soundness bank examinations. The examiner should document any findings, especially those which do not satisfy the recommendations in *1996 FFIEC IS Examination Handbook*.

Tier I

GENERAL

1. Obtain or prepare a description of all wholesale EFT applications employed by the institution.

2. For each identified EFT application, obtain or prepare an organization chart.

3. Determine the adequacy of insurance coverage for each EFT operation and the overall EFT environment.

4. Review the minutes of management committees responsible for overall or any specific EFT activity for content and follow-up of any material matters set forth.

WHOLESALE OR LARGE DOLLAR FUNDS TRANSFER SYSTEMS (FTS)

5. Obtain or prepare a flowchart (or detailed narrative) of the overall FTS. Review the information to determine the degree of automated interface, linkage to functions not supported by the FTS and separation of duties/functions considering:

   a. Fedwire.
   b. CHIPS or other local payments system.
   c. SWIFT.
   d. Telex.
   e. Internal transfers (book entry).
   f. Customer networks.
   g Internal networks.

h. Other payment origination sources (e.g., telephone, fax, mail, internal memos, standing instructions).

i. Testing of payment origination messages.

6. Review policies and procedures in place to monitor customer balances for outgoing payments to ensure that payments are made against collected funds or established intraday or overnight overdraft limits and that payments resulting in excesses of established uncollected or overdraft limits are properly authorized.

7. Review the adequacy of security procedures in place for both outgoing and incoming payment orders for each step of the FTS process considering:

   a. Payment order origination (e.g., message testing for telex, telephone, letters/memos, fax).

   b. Data entry.

   c. Payment order execution/release.

   d. Telecommunications lines.

   e. Physical security.

8. Review a sample of contracts authorizing the institution to make payments from a customers account to ensure that they adequately set forth responsibilities of the institution and the customer, primarily regarding provisions of the Uniform Commercial Code Article 4A (UCC4A) related to authenticity and timing of transfer requests.

9. Review the disaster recovery plan for the FTS to ensure that it is reasonable in relation to the volume of activity and that all units of the FTS are provided for in the plan and regularly tested. Consider the CHIPS requirement for participants that originate more than $20 billion daily transfer value for Fedwire and CHIPS combined.

10. Review the audit program to ensure all functions of the FTS are covered, including:

a. Payment order origination (funds transfer requests).

b. Message testing.

c. Customer agreements.

d. Payment processing and accounting.

e. Personnel policies.

f. Physical and data security.

g. Contingency plans.

h. Credit evaluation and approval.

i. Incoming funds transfers.

j. Bank Secrecy and OFAC issues.

k. Federal Reserve's Payment Systems Risk Program.

11. Compare the last executed internal audit procedures covering each of the areas noted in step 10 above, to the related questions detailed in Tier II of these procedures, and determine whether they meet or exceed Tier II coverage.

12. Review a sufficient sample of supporting audit workpapers necessary to confirm that they support the execution of procedures established in step 11 above.

13. Review all audit reports related to the FTS and determine the current status of any exceptions noted in the audit report.

BSA and OFAC REVIEW

14. Determine if the wire transfer area maintains reports to identify potential money laundering activities (BSA).

15. Determine if the wire transfer area maintains OFAC identification and reporting capabilities.

16. If there are any shortfalls in identification or recordkeeping under steps 14 or 15 above refer to the EIC and/or your agencies Compliance/BSA subject matter expert(s) (SME).

17. Consistent with the scope of the examination, procedures included in Tier II that are not sufficiently covered under steps 11 and 12, above, are to be implemented as part of this examination . (Note: To the extent coverage is clearly satisfactory and current, audit procedures and workpapers also may be used to address steps 6 through 9).

CONCLUSIONS

18. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

19. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

20. Assign rating. (See the Chapter 5 for additional information.)

21. Prepare an index of workpapers for this section of the workprogram.

22. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable,

recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

23. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date
_____|_____

Reviewer's Initials

Tier I Addendum
FEDWIRE THIRD-PARTY ACCESS ARRANGEMENTS

The following procedures should be used, as appropriate

The Federal Reserve Board allows, under certa in conditions, a depository institution (the participant) to designate another depository institution or entity (the service provider) to in itiate, receive or otherwise process Fedwire funds transfers and book-entry securities transfers that are posted to its reserve or clearing account held at the Federal Reserve Bank. Such third-party access arrangements are permitted providing the specific conditions outlined in section G of the Federal Reserve Policy Statement on Payments System Risk (FRRS 9-1016) have been met. If Fedwire funds and/or book-entry securities transfer operations are performed by a service provider:

1. Ensure that the participant retains control o f the credit-granting process by individuall y approving each funds/securities transfer o r establishing individua l customer transfer limits and a transfer limit for the participant's ow n activity, within which the service provider can act.

2. Determine whether the service provider:

   a. Obtains the participant's permission to initiate transfers that would exceed individual customer credit limits or the transfer limit for the participant's own activity.

   b. Notifies the participant of incoming book-entry securities transfers that exceed the applicable limit, and determine that the participant's instructions to accept or reverse the transfer are processed by the service provider in a timely manner.

3. Determine whether:

   a. All Fedwire transfer activity is posted to the participant's account and that the institution maintains responsibility for its account.

   b. Participant has the ability to monitor transfer activity conducted on its behalf.

4. Determine if the participant's board of directors has approved the following:

   a. The role and responsibilities of a service provider (that is not affiliated with the participant through at least 80 percent common ownership).

   b. That in a L/C arrangement, the intraday overdraft limit for the activity to be processed by the service provider and the credit limits for any inter-affiliate funds transfers.

5. Assess whether the participant has adequate contingency backup capabilities for its transfer activities as set forth in the *Interagency Policy On Contingency Planning for Financial Institutions, FFIEC SP-5.*

6. For arrangements where the service provider is not affiliated with the participant through at least 80 percent common ownership, determine that the participant is able to continue Fedwire operations if the participant is unable to continue its service provider arrangement in the event the participant's primary supervisor terminated the arrangement.

7. Determine if the participant has certified that the arrangement is consistent with corporate separateness and does not violate branching restrictions.

8. Assess whether the participant has certified that the arrangement will allow the participant to comply with all applicable state and federal laws and regulations governing the participant, including retaining and making accessible records in accordance with the regulations adopted under the Bank Secrecy Act.

9. Determine if the participant's primary supervisor has affirmatively stated in writing that it does not object to the arrangement.

10. Determine whether:

    a. Ensure that the participant has in place an adequate audit program to review the third-party access arrangement at least annually.

    b. In the case of an arrangement involving a foreign service provider,

ensure that the participant and the service provider have in place an adequate audit program that addresses Fedwire operations and that reports are made available to the Federal Reserve and the participant's primary U. S. supervisor(s) in English. (This program should confirm compliance with the provisions stipulated in section G of the Federal Reserve Board's Payments System Risk Policy.)

11. Assess whether the service provider is subject to examination by the appropriate federal depository institution regulatory agency(s).

12. Determine if the participant and the service provider(s) have executed an agreement with the relevant Reserve Bank(s) incorporating the conditions stipulated in the Fedwire third-party access policy.

CONCLUSIONS

13. Proceed to procedure 18, Tier 1.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

Negative response/determinations should be discussed with , management , their remedy, compensating controls and the examiner's comments should be recorded in the workpapers.

WHOLESALE OR LARGE DOLLAR FUNDS TRANSFER SYSTEMS

Funds transfer requests

1. Does the funds transfer function maintain a current list of bank personnel authorized to initiate transfer requests?

2. Does the bank limit the number of employees who can initiate or authorize transfer requests?

3. Are authorized employee signature records kept in a secure environment?

4. Are standard, sequentially numbered, forms used by bank personnel to initiate funds transfer requests?

5. If standard forms are not used in certain circumstances (e.g., telephone requests from remote offices) is an authentication system used?

6. Does the bank employ an adequate security procedure for requests received from customers via telex, on-line terminals, telephone, fax, or written instructions?

7. Is more than signature verification (e.g., tests, call backs) required on written requests (e.g. memos, letters, fax)?

8. Does the bank maintain a current record of authorized signers for customers who use the bank's funds transfer services and does it include authorized sources (e.g., telephone, memo, fax)?

9. Does the bank advise its customers to limit the number of authorized signers?

10. Are customer signature records maintained under dual control or otherwise protected?

	Comments
11. Do customer authorization lists limit the amount that an individual is authorized to transfer?	
12. Has the bank established guidelines for what information should be obtained from a person making a funds transfer request?	
13. Do the records of transfer requests contain:	
a. The account title and number?	
b. A sequence number?	
c. The amount to be transferred?	
d. The person or other source initiating the request?	
e. The time and date?	
f. Authentication?	
g. Paying instructions?	
h. Bank personnel authorizing certain types and dollar amount transfers?	
14. Does the bank have procedures in effect to prohibit persons who receive transfer requests from transmitting or accounting for those requests?	
15. Does the bank use devices that record all incoming and outgoing telephone transfer requests?	
16. If calls are recorded, does the bank advise its customers in written contracts, by audible bleeping signals, or by informing the caller that telephone calls are being recorded?	
17. Does the funds transfer function maintain sequence control internally for requests that it processes?	

18. Are incoming and outgoing messages time stamped or sequentially numbered for control?

19. Are transfer requests recorded in a log or another bank record before execution?

20. Is the log or record of transfer requests reviewed daily by supervisory personnel?

21. If not sequentially accounted for, is an unbroken copy of all messages received via telex or other terminal printers kept throughout the business day?

22. Are sequence records and unbroken copies reviewed and controlled by someone not connected with equipment operations?

TEST KEYS

23. If test keys are used for authentication, are the files containing test key formulas maintained under dual control or otherwise protected?

24. Are only authorized personnel permitted in the test key area or allowed access to terminals used for test key purposes?

25. Does the bank maintain an up-to-date test key file?

26. Does management maintain a list of those persons who have access to test key files?

27. Are all messages and transfer requests that require testing authenticated by the use of a test key?

28. Are test codes verified by someone other than the person receiving the initial transfer request?

29. Does the bank's test key formula incorporate a variable (e.g., sequence number) and is the requirement stated in an agreement between the bank and the customer?

30. Does the bank have procedures in operation for the issuance and cancellation of test keys?

31. Is the responsibility for issuing and canceling test keys assigned to someone who is not responsible for testing the authenticity of transfer requests?

AGREEMENTS

32. Are agreements in effect concerning funds transfer operations between the financial institution and its customers, correspondent banks, systems providers (e.g., Federal Reserve Bank and CHIPS), servicers, and hardware/software vendors?

33. Do the agreements fix responsibilities and accountability between all parties?

34. Do agreements with customers adequately describe the security procedures as defined by UCC Article 4A Sections 201 and 202?

35. Does the bank obtain written waivers from its customers if they chose security procedures that are different from what is offered by the bank, as indicated in UCC Article 4A Section 202(c)?

36. Do agreements with customers establish cut-off times for receipt and processing of payment orders and canceling or amending payment orders as noted in UCC Article 4A Section 106?

PAYMENT PROCESSING AND ACCOUNTING

37. Does the funds transfer department of the bank prepare a daily reconcilement of funds transfer activity (incoming and outgoing) by dollar amount and number of messages?

38. Does the funds transfer department perform end-of-day reconcilements for messages sent to and received from intermediaries (e.g., Federal Reserve Bank, servicers, correspondents, and clearing facilities)?

39. Are all pre-numbered forms, including cancellations, accounted for in the daily reconcilement?

40. Are reconcilements of funds transfer and message requests reviewed daily by supervisory personnel?

41. Is the balancing of the daily activity separate from the receiving, processing, and sending functions?

42. Does the funds transfer department verify that work sent to and received from other bank departments agrees with its totals?

43. Is someone responsible for reviewing all transfer requests to determine that they have been properly processed?

44. Are key fields reverified before transmission and are messages released by someone other than the individual originally entering the message?

45. Are all rejects and/or exceptions reviewed by someone not involved in the receipt, preparation, or transmittal of funds?

46. If the institution accepts transfer requests after the close of business or transfer requests with a future value date, are they properly controlled and processed?

47. Are Federal Reserve Bank, correspondent bank and clearing house statements used for funds transfer activities reconciled and reviewed daily in another area of the bank (e.g., accounting or correspondent banking) to determine that they agree with the funds transfer departments records and the reasons for any *open* funds transfer items?

48. Are open statement items, suspense accounts, receivables/payables, and inter-office accounts related to funds transfer activity controlled outside of the funds transfer operations?

49. Are periodic reports on open statement items, suspense accounts and inter-office accounts prepared for management and do the reports include aging of open items, the status of significant items and resolution of prior significant items?

50. Are corrections, overrides, open items, reversals, and other adjustments reviewed and approved by an officer?

51. Are all general ledger tickets, or other supporting documents initialed by the originator and supervisory personnel?

52. Does the bank maintain adequate records as required by the Currency and Foreign Transactions Reporting Act of 1970 (also known as the Bank Secrecy Act)?

PERSONNEL

53. Has the bank taken steps to ensure that screening procedures are applied to personnel hired for sensitive positions in the funds transfer department?

54. Does the bank prohibit new employees from working in sensitive areas of the funds transfer operation unless they are closely supervised?

55. Are temporary employees excluded from working in sensitive areas? If not, is the number of such employees limited and are they closely supervised?

56. Are statements of indebtedness required of employees in sensitive positions of the funds transfer function?

57. Are employees subject to unannounced rotation of responsibilities?

58. Are relatives of employees in the funds transfer function precluded from working in the same institution's bookkeeping, audit and data processing functions, and/or in departments generating funds transfer requests?

59. Does the bank's policy require that employees take a minimum number of consecutive days as part of their annual vacation and is the policy being enforced?

60. Does management reassign employees who have given notice of resignation or have been given termination notices, from sensitive areas of the funds transfer function?

PHYSICAL AND DATA SECURITY

61. Is access to the funds transfer area restricted to authorized personnel?

62. Are visitors to the funds transfer area identified, required to sign in, and be accompanied at all times?

63. Is written authorization by department management given to those employees who remain in the funds transfer area after normal working hours and are security guards informed?

64. Are bank terminal operators or others in funds transfer operations denied access to computer equipment areas or programs?

65. Do procedures prohibit computer personnel from gaining access to bank terminals or test key information used for funds transfers?

66. Does funds transfer equipment have physical and/or software locks to prohibit access by unauthorized personnel at all times?

67. Are terminals and other hardware in the funds transfer area shut down after normal working hours and or regulated by automatic time-out controls or time-of-day controls?

68. Are passwords suppressed on terminals when being entered?

69. Are operator passwords changed and, if so, are they changed at reasonable intervals?

70. Is supervisory approval required for terminal access made at other than authorized times?

71. Are passwords restricted to different levels of activity (e.g., input, release, and adjustments) and to data files?

72. Is terminal operator training conducted in a manner that will not jeopardize the integrity of live data or memo files?

73. Are employees prohibited from taking keys for sensitive equipment out of the funds transfer area?

74. Does the bank maintain back-up systems for events such as equipment failures and line malfunctions?

75. Are back-up systems periodically tested by bank personnel?

76. Does the use of back-up equipment require approval by supervisory personnel?

77. Are procedures and controls in place to prevent the inadvertent release of test data into the production environment, thus transferring live funds over the system?

CONTINGENCY PLANS

78. Have written contingency plans been developed for partial or complete failure of the systems and/or communication lines between the bank and correspondent bank, servicer, CHIPS, Federal Reserve Bank, and data centers. Do the procedures, at a minimum, ensure recovery by the opening of the next day's processing?

79. Are these contingency plans reviewed regularly and tested periodically?

80. Has management distributed these plans to all funds transfer personnel?

81. Are sensitive information and equipment adequately secured before evacuation in an emergency and is further access to the affected areas denied by security personnel?

CREDIT EVALUATION AND APPROVAL

82. Does the funds transfer department or another area of the bank have procedures in effect to prohibit transfers of funds against accounts that do not have collected balances or preauthorized credit availability?

83. Have customer limits been established for intraday and overnight overdrafts?

    a. Are groups of affiliated customers included in such limits?

    b. Are funds transfers activities monitored during the business day to ensure that payments

causing limits to be exceeded are not executed without proper approval?

c. Are the limits reviewed and updated?

d. Are the customer limits revised by senior management at reasonable intervals?

84. Does the bank make payments in anticipation of the receipt of covering funds? If so, are such payments approved by officers with appropriate credit authority?

85. Are intraday exposures limited to amounts expected to be received the same day?

86. Are intraday overdraft limits established giving consideration to other types of credit facilities for the same customer?

87. Is an intraday record kept for each customer showing opening collected and uncollected balances, transfers in and out, and the collected balances at the time payments are released?

88. If payments exceed the established limits, are they referred to a person(s) with appropriate credit authority before releasing payments and steps taken in a timely manner to obtain covering funds?

89. When an overnight overdraft limit is exceeded, is a determination made as to whether a fail caused the overdraft? If so, is this properly documented? Is adequate follow-up made to obtain the covering funds in a timely manner?

90. Where required as a participant of a net settlement system (e.g., CHIPS), are bi-lateral credit limits set based on a formal credit analysis and are the limits approved by the appropriate level of management?

91. If the institution is an Edge Act corporation do intraday and overnight overdrafts comply with Regulation K?

INCOMING FUNDS TRANSFERS

92. Are incoming payments not received over a secure system (e.g., Fedwire), such as book entry

transfer requests received via telex or phone, authenticated prior to processing?

93. Are separation of duties maintained over receipt of instructions, posting to a customers account, and mailing of customer credit advices?

94. Are audit trails maintained from receipt through posting to a customers account?

95. Is issuance of customer advices timely?

96. Are incoming credits accurately accounted for throughout the process?

PAYMENT SYSTEM RISK

97. If the institution incurs overdrafts in its Federal Reserve Account, has the Payment System Risk program been completed (i.e., has the institution selected an appropriate net debit cap)?

98. If the institution has elected a de minimis or self-assessment net debit cap, ensure that the examination evaluates the adequacy of records supporting the institution's program and accuracy of the de minimis or self-assessment rating.

POLICY AND STANDARDS

99. Do standards exist for:

    a. Software and hardware *acquisition* including:

        1) Cost benefit analysis?
        2) Programming standards?
        3) Documentation Standards?
        4) Ownership of programs, spreadsheets, etc. developed on the institution's time and equipment?
        5) Escrow of source code of critical, tailor-made funds transfer software to ensure the institution can continue to maintain software in event of failure of vendor?

    b. Micro/mini computer use including:

        1) Use of the output/data?
        2) Restrictions on personal and nonjob related use?

3) Use of personal equipment and/or software?
4) Use of unauthorized software?
5) Modification of the hardware and or software?
6) Copying or piracy of the software?
7) File backup?

100. Have housekeeping procedures been developed and enforced to provide protection from:

a. Food?

b. Liquids?

c. Dust, smoke?

d. Magnetic fields?

101. Have procedures been developed and enforced for:

a. Backup and off-site storage of critical information?

b. Inventory control on the hardware software?

102. Have adequate security measures been established covering:

a. Physical security.

1) Restricted area.
2) Key locks on the machines.
3) Removing and securing the data files.

b. Access controls.

1) Passwords.
2) Encryption of data on the disk.
3) Use of dial-up equipment.
4) Read only attributes to the files.

103. Proceed to procedure 18, Tier I.

Examiner | Date

_____|_____

Reviewer's Initials

FEDLINE EFT CHAPTER 19

(FILE NAME ON DISK # 2 = S2C19.WPD)

This section is designed specifically to address the proper setup of terminal related security for the Federal Reserve Fedline terminals. It covers only the wire transfer function of Fedline. A number of other security and control issues surround the wire transfer function, including balancing functions, reviewing Fedline activity logs, separation of duties, credit limits, collected balances, transferee identification, etc. These items may be reviewed through reference to Chapter 18, Wholesale EFT.

LOCAL SECURITY ADMINISTRATOR

The Local Security Administrator (LSA) is responsible for setting up new users on the local Fedline system. The LSA also is responsible for setting the function levels of all users. The LSA is a powerful user and has the tools to bypass all security and effectively send a transfer with no supervision, if other compensating controls, such as prompt balancing and timely activity log review, are not in effect. Internal controls and proper separation of duties are important in protecting the bank from significant risk.

The LSA should be someone in the bank who has *NO* day-to-day operational duties on the Fedline terminal. The LSA's main purpose should be to add new users and change function security levels. Anytime the LSA uses the terminal, a member of the daily operations staff should be present to monitor his/her actions. If the Fedline terminal has a power on password, it should be implemented and the password restricted from the LSA. In addition, the LSA should not have a host access logon at the Federal Reserve host mainframe computer. This would prevent the LSA from logging onto the host mainframe and sending a transfer immediately. However, the LSA could queue the transfer (TQ status), and the next time a valid transfer exchange was made, the unauthorized transfer would be sent in that batch. However, this method increases the chances that an unauthorized transfer would be detected.

The LSA with unrestricted access could perform the following functions to bypass security:

- Add two new user IDs having enter and verify capability and enter a transfer.
- Change the verification rule to N, thus eliminating the verification requirement.
- Change the verification threshold dollar amount to $99,999,999.99, thus circumventing verification.

Accordingly, these functions must be controlled.

MISCELLANEOUS SECURITY SETTINGS

User ID suspended – Consecutive bad password retries – Specifies the maximum number of consecutive invalid sign-on attempts operators can make before the local user ID is suspended. This prevents an unauthorized person from trying to guess the password of a legitimate user by limiting the number of invalid password retries. The Federal Reserve Board's recommended setting is 3.

Users must periodically change their password every XX days – Specifies the maximum number of days operators can use their password before they must change it. The Federal Reserve Board's recommended setting is 30.

Verification rule – This rule sets the message verification requirement. This prevents the origination of unauthorized (fraudulent) messages. This rule should require that more than one person be involved with the processing of transfers. Three options are available, N, U, and E (see the description of the option settings below). The Federal Reserve Board's recommended setting is E, however U is acceptable. (Note: This rule will affect all the types of message transactions that require verification; such as funds transfer, large dollar check returns and TT&L.)

Options:

- *N – No restriction (Very high risk)* – This option allows the operator who entered and/or updated a

message also to verify that same message. There is no dual control of any wire transfers if this option is chosen. For example, Mary enters a message. She also can update and verify that same message.

- *U – Verifying operator cannot be the last operator who updated the transfer*. This option prevents the last operator who entered or updated a transfer from verifying that same message. It would allow the original operator to verify the transfer if it was changed by a second operator. For example, Mary enters a transfer and Paul updates (changes) that same message. Paul cannot verify that same message, but Mary can.

- *E – Verifying operator cannot be operator who entered or updated the transfer*. This option prevents any operator who entered or updated a transfer from verifying that same transfer. For example, Mary enters a transfer and Paul updates that same transfer. Neither Mary nor Paul can verify that same message. Some other Fedline operator who has verify access must verify the transfer.

Override and release rule – This field is used to indicate the level of restrictions placed on overriding and/or releasing transfers. This potentially allows users to bypass verification. Only operators with the *supervisor function* access level have the ability to perform the Override & release function. The Federal Reserve Board's recommended setting is E, however U is acceptable.

- *N – No restriction on override or release –* Any operator with the supervisor function access level can override or release the verification of a transfer regardless of any previous processing performed with the exception of messages that have a status of TQ, MC, or CN.

- *U – Limited restriction on override or release –* The operator overriding or releasing the transfer cannot be the operator who last updated the message.

- *E – Full restriction –* The operator overriding or releasing the transfer cannot be the operator who updated or entered the message.

Timeout Intervals – This timeout parameter minimizes the amount of time that a terminal remains active if a user forgets to sign-off. It causes the system to revert to the Fedline Sign-on screen after a specified amount of time during which no keystrokes have been entered at the PC. The Federal Reserve Board's recommended setting is 10 minutes.

Cycle-Date rollover and Print-delete option – This option allows the bank to select the type of report to be printed to document the previous day's wires that were queued for transmission, but were not sent, before they are deleted from the Fedline system. The software ships with FULL as the default.

- *FULL –* Prints a full recap report of the previous days wire transfers before they are deleted by the cleanup cycle date mode change program.

- *SUMMARY –* Prints an abbreviated report of the previous days wire transfers before they are deleted by the cleanup cycle date mode change program.

USER/ACCESS REPORT EVALUATION

Staff member(s) assigned the Local Security Administrator (LSA) function should be restricted from the funds transfer (FT) application. LSAs should not have access to the FT application. If the FT application is listed, it may indicate that the LSA is involved in ongoing funds transfer activity.

Staff member(s) assigned the LSA function should be restricted from the Host Communications (HC) function. A staff member with HC access could log on to the Federal Reserve host mainframe and transmit the wire transfer. (Note: The staff member must have a host logon ID and security access on the Federal Reserve host mainframe to implement the wire transfer. There is no way to determine on-site at the bank if a user has host access. This only can be determined by calling the data security department of the Federal Reserve Bank. The listing or non-listing of the HC application under the user's ID is usually a good indicator of their host access ability. However, this method of determination is not conclusive since the LSA can use the *Master ID* to activate this application at any time.)

The Local Security Administrator (LSA) should be

assigned *only* the Local Administration (LA) application. Since the LSA should not be involved in the daily ongoing operation of the Fedline terminal. There is no reason for them to have access privileges to any other available applications other than LA.

Staff members should have no more than one user ID. Staff members with more than one user ID can by-pass the verification requirement by signing on with the first ID to enter transactions and then signing on with the second ID to perform the verification.

No more than two staff members should be assigned as Local Security Administrators. Local Administrator access is very powerful and therefore its use should be limited as much as possible. The Federal Reserve guidelines suggest an Administrator and one backup Administrator. Depending on the size of the institution, the existence of more than two staff members with Local Administrator capabilities should be criticized.

No staff members should have the funds transfer (FT) Supervisor or Manager function. These functions have funds transfer access levels that provide the ability to bypass the verification requirement. These access levels should only be activated by the Local Security Administrator in unusual circumstances. The Local Security Administrator should monitor the actions performed using these access levels and then deactivate these levels when the action is complete. It is possible that the Supervisor function is needed in other applications such as *Startup/Shutdown Control*. However, it is not normally needed in the funds transfer application.

No staff members other than the Local Security Administrator should have the Local Administration (LA) application priviledge. Verify that the staff members who operate the Fedline on a daily ongoing basis do not have the LA privilege listed under their user ID on the *User/Access report*. The ** listing grants access to all applications listed on the menu except the LA function. Therefore, the ** could be appropriate depending on the circumstances. The LA function will be specifically listed if the user has access to this application and should be criticized accordingly.

VERIFICATION FIELDS

The update funds application attributes option allows the staff members with Manager function level or the LSA to set the verification fields for wire transfers.

Available options range from no verification of any field to required verification of every field. In between these two extremes, the Manager or LSA can select individual fields that would require second operator verification. Verification refers to fields which must be re-keyed by a second operator. If none of the fields have an X next to them, no re-keying is required by the second operator. However, a second operator will still have to provide a sight verification by calling up the transfer on the screen and reviewing it. The Federal Reserve Board recommends that, at a minimum, verification of the dollar field should be required, (i.e., marked with an X to indicate that a second operator will have to rekey in the dollar amount). Some banks might choose additional fields to verify, such as, account number, routing number, etc.

VERIFICATION THRESHOLD

The update funds application attributes option allows the staff members with Manager function level to set the verification threshold for wire transfers.

Available options range from no verification of any transfers required to verification of every transfer required. In between these two extremes, dollar-floor limits also are available.

Normally, a bank should set the verify threshold to $0.00 which requires verification of all transfers by a second operator. If the bank should decide to set the verification level at a higher amount, this amount should be approved by the Board of Directors and noted in the minutes. (Note: an amount of $99,999,999,999.99 in the verify threshold field indicates that the requirement for verification by a second operator has been turned off.)

GENERAL CONTROLS

Master password backup storage – There might be a situation where a local administration function needs to be performed, but there are no Local Security Administrators available. Therefore, the Master User ID password should be stored in a secure location and be available for the operating personnel should the need arise. The Master User ID password should be changed by the LSA after it is used by the operating personnel.

Fedline configuration diskette – The diskette is used by the bank in conjunction with the Federal Reserve in case everyone is locked out of the system. The Fedline configuration diskette should be securely stored.

PC power-on password – Many microcomputers have the ability to activate a power-on password feature. This feature forces the input of a password before the computer will activate. If the Fedline terminal has this feature available, it should be activated. The Local Security Administrator(s) should not have access to this password. This control will prevent an LSA from entering transfer requests when the terminal is not monitored by operating personnel.

DISASTER /CONTINGENCY

Recovering wire transfer operations in a disaster situation is an operational concern. Generally, unless the bank sends and receives many transfers, the telephone can be used as a backup method. The wire transfer personnel should know where the current backup code word list is stored. Wire transfer terminals are standard PCs with a Federal Reserve issued encryption board. Turnaround time for acquiring new equipment should be fairly rapid.

The bank should be queried as to what its contingency plans are in the event of an equipment failure (e.g., encryption device failure) or the loss of the Fedline terminal(s). The banks contingency plan should include keeping a backup copy of the current version of the Fedline software available on diskette and periodically making a static file backup of the Fedline (backup static files function in the miscellaneous support application) application that will copy all customized data used by the bank (e.g., frequent ABA's, User ID's, and recurring transfers).

FEDWIRE WIRE TRANSFER FUNCTIONS

The following reflect Fedwire functions along with a brief description.

Entry/Update

- Create a message – Enter a transfer.
- Derive a reversal – Reverse a previously received transfer.
- Export a message file – Copy selected funds transfers onto a diskette.
- Import a message file – Copy funds transfers created using another processing system into Fedline.
- Update a message – Change detail information in a transfer.

Verify/Transmit

- Group release – Change status of a group of transactions for immediate release.
- Release transfers for transmit – Change status of transfer marked "held" to release.
- Verify a message – Verify a previously entered transfer.

Asst. Supervisory functions

- Add recurring template – Create new template.
- Delete recurring template – Delete template.
- Update recurring template – Modify template.

Supervisory functions

- Group override – Change status of a group of messages held from transmission.
- Message status override – Allows the status of a transfer to be changed (by-passes any verification).
- Modify screen defaults – Allows you to modify default data of the create screens which are automatically inserted whenever you create a message.
- Re-send message – Allows you to resend a previously transmitted message that may have been lost by the receiver or rejected by the host.

Managerial functions

- Resync. host – resequence transfer ID appl seq# numbers on Fed main frame.
- Update key verify – select fields in transfer fields entry that must be verified.
- Update application – specify dollar amount attributes of outgoing transfers that require verification.

This section is intended to determine the adequacy of controls over the specific Fedline EFT activities of the organization. Although these applications should operate outside the IS environment, they are highly dependent on computer operations. The procedures are created so that they may be implemented separately as part of either the IS examination or safety and soundness examinations. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*. There are no Tier II procedures in this workprogram. (Note: Even though some of the keystrokes are provided as examples, the examiner should never obtain the information identified directly from the terminal. Rather, the examiner must always request such information from the institution.)

GENERAL

1. Obtain a screen print of the miscellaneous security settings screen (option #99 on LA menu).

2. Obtain a User-ID Status Report (option #60 on LA menu – type all to get all users).

3. Obtain a User/Access Report (option #65 on LA menu – press enter key for all users).

4. Obtain a screen print of the verify fields screens (option #93 on FT menu of manager) (structured, structured draw down and non-structured).

5. Obtain a screen print of the verify threshold screen (option #96 on FT menu of manager)

FEDLINE WIRE TRANSFER APPLICATION

6. Are the miscellaneous security settings set correctly (refer to step 1) and:

   a. Will the user ID be suspended after three or less tries?

   b. Must the user change his/her password every 30 days or less?

   c. Is the verification rule set to E or U?

   d. Is the override and release rule set to E or U?

   e. Is the timeout interval set to 10 minutes or less?

7. Does the User/Access Report (refer to step 3.):

    a. Show that the staff member(s) assigned as Local Security Administrator has (have) the proper LA application security setup and:

        1) Is the staff member(s) assigned the LA application restricted from the funds transfer (FT) application?

        2) Is the staff member(s) assigned the LA application restricted from the host communications (HC) function?

        3) Is the staff member(s) assigned the LA application restricted to *only* the LA application?

    b. Show that no one has more than one user ID.

    c. Show that there are no more than two staff members assigned as local security administrators?

    d. Show that no one has the funds transfer supervisor or manager function on a continuing basis?

    e. Show that no one other than the Local Security Administrator(s) has (have) the LA application?

8. Do the three verify screens show (refer to #4 above):

    a. An X in the amount field?

9. Does the verify threshold screen reflect (refer to #5 above):

    a. The verify threshold set to 0.00?

    b. If the verify threshold is greater than 0, that the amount has been approved by the board of directors and noted in the board minutes?

10. Is the Master User ID password stored in a sealed envelope in a secure location in case the Local Security Administrator(s) is (are) not available?
11. Is the Fedline *configuration diskette* stored in a secure location and available only to the Local Security Administrator?

12. Does the Fedline terminal have a power-on pass word option? If yes:

    a. Is it activated?

    b. Is this password restricted from the Local Security Administrator(s)?

13. Disaster/Contingency Plan

    a. Does the bank have a method for sending/receiving wire transfers in the event of equipment failure?

    b. Does the bank have a method for sending/receiving transfers if they must operate at a different site?

    c. Does the bank keep a copy of the current version of the Fedline software available on diskette?

    d. Does the bank periodically make a static file backup of the Fedline software?

CONCLUSIONS

14. Review the results of work performed in this chapter and in chapters for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies reach a conclusion. Workpapers should reflect the examiner's review process.

15. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

16. Assign rating (see Chapter 5 for additional information).

17. Prepare an index of workpapers for this section of the workprogram.

	Comments
18. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.	

Examiner | Date

_____|_____

Reviewer's Initials

RETAIL EFT (ATM AND POS) CHAPTER 20

(FILE NAME ON DISK # 2 = S2C20.WPD)

Automation has enabled banks to electronically perform many retail banking functions formerly handled manually by tellers, bookkeepers, data entry clerks and other banking personnel. Examples of retail Electronic Funds Transfer (EFT) systems include automated teller machines (ATM), point-of-sale (POS) networks, debit and smart cards, and home banking. Accordingly, the need for physical banking facilities and related staff has been reduced. EFT and related banking services also has brought access to, and control of, accounts closer to the consumer through use of widely distributed unstaffed terminals and merchant facilities. EFT related risk to a financial institution for individual customer transactions is generally low, since the transactions are usually for relatively small amounts. However, weaknesses in controls that could lead to incorrect or improper use of several accounts could lead to significant losses or class action suits to a financial institution. Examinations of retail EFT facilities should focus on the potential large scale risks of a given product.

As with other EFT services, financial institutions have found it beneficial to share their ATM and POS systems' costs and realize economies of scale. This has led some institutions to form alliances that are mutually beneficial. Two examples are:

- Shared systems – A group of financial institutions mutually research, install, market and operate the system.

- Interchange systems – Separate institutions with ATM programs or separate shared systems allow each other's customers use of their machines.

Additionally, there are single institution systems, where only the customers of the bank that developed and installed the ATM system may use the machine.

Fraud, robbery and malfunction are the major risks in an ATM environment. Although the use of plastic cards and PINs act as a deterrent, there is a risk that an unauthorized individual may obtain them. Customers even may be physically accosted while making withdrawals or deposits at ATM locations. Some institutions have decreased this risk by installing surveillance cameras and access/entry control devices.

AUTOMATED TELLER MACHINES (ATM)

An ATM is an EFT terminal that is capable of performing many routine banking services for the customer. ATMs handle deposits, transfers between savings and checking accounts, balance inquiries, withdrawals, small short-term loans and payments to third parties. ATMs usually operate 24 hours a day and are located both on and off bank premises. Daily withdrawals are normally limited to relatively small amounts (usually $500 or less). Deposits are processed in the same manner as if handled by a teller.

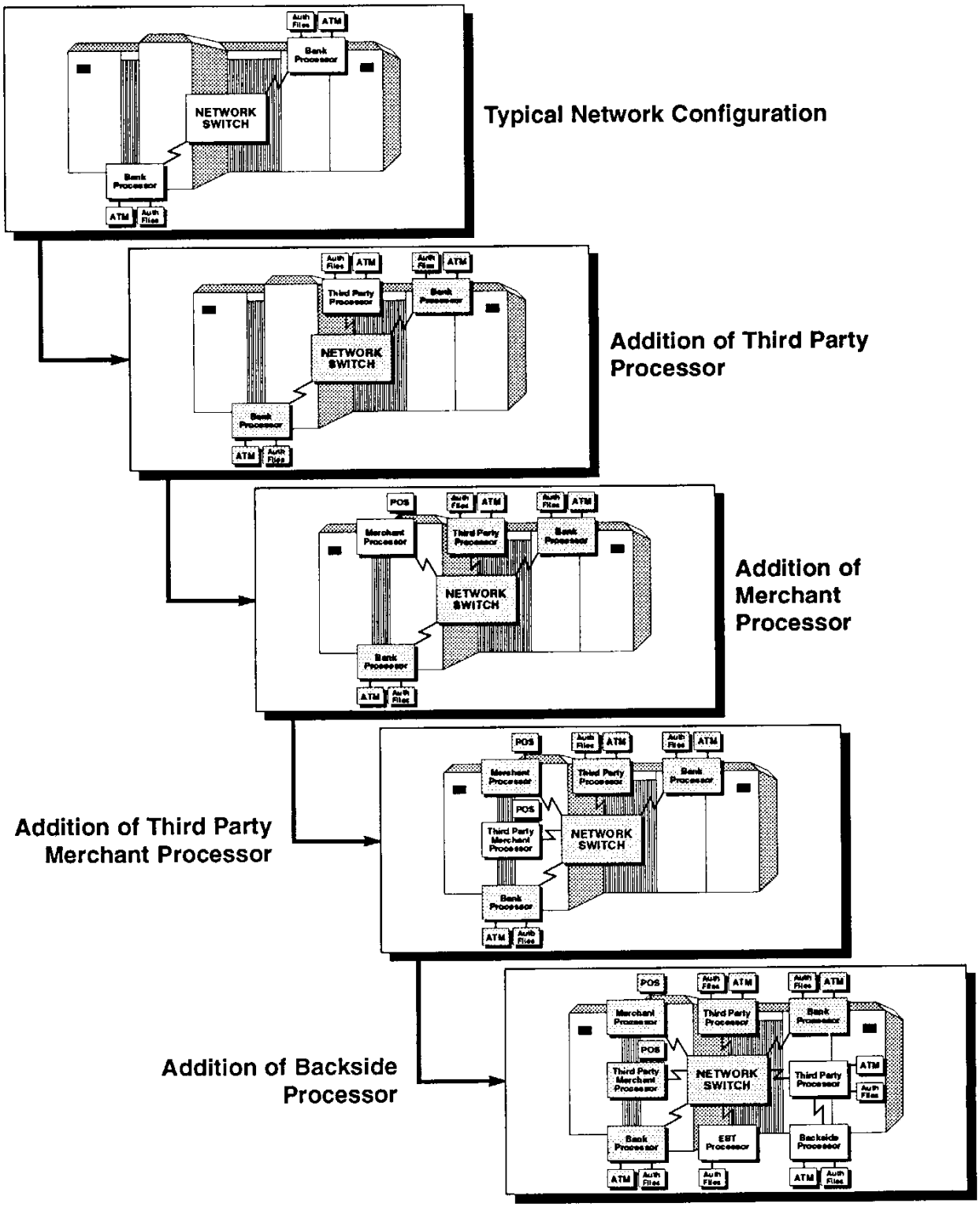
ATMs are generally activated through use of a plastic card encoded with a machine readable customer identification number. In most systems, the customer is required to enter a corresponding personal identification number (PIN).

ATM machines operate in either off-line or on-line mode. Off-line transactions are recorded on tape and physically transported to the financial institution for daily processing. Since off-line systems are not directly connected to the financial institution's computer system, balance verification is normally limited to the customer's opening balance. On-line systems are directly connected to a financial institution's computer system. The computer processes each transaction immediately and provides instant account balance verification. On either system, a card is normally captured if misuse is indicated (e.g., reported stolen or improper PIN number).

POINT-OF-SALE SYSTEMS (POS)

A POS system transaction is defined as an electronic transfer of funds from a customer's checking or savings account to a merchant's account to pay for goods or services. Transactions are initiated from

Figure 20.1
ATM Networks Continue to Increase in Complexity



With Permission S. Paur, Pulse EFT Association

POS terminals located in department stores, supermarkets, gasoline stations, and other retail outlets. In an electronic POS system, a customer pays for purchases using a plastic card (e.g., ATM card or debit card). The store clerk enters the payment information into the POS terminal and the customer verifies the transaction by entering a PIN. This results in an automatic debit to the customer's account and credit the merchant.

POS transactions may either be processed through single-institution unshared systems or multi-institution shared networks. Participants in a shared systems settle daily, on a net transaction basis, between each other. In unshared systems, the merchants and customers have accounts with the same financial institution. Thus, the need to settle for transfer of funds between banks is eliminated.

As with other EFT systems, POS transactions are subject to risk of loss due to fraud, mistakes, and system malfunction. POS fraud is caused by stolen cards and PINs, counterfeit cards, and direct computer access. The system also is susceptible to errors such as debiting or crediting an account by too much or too little and entering unauthorized transactions. For the most part, POS systems usually deal with these risks by executing bank-merchant and bank-customer contracts that delineate each party's liabilities and responsibilities. Also, consumers are protected by state and federal statutes limiting their liability if they give notice of a lost, stolen or mutilated card within a specified time period. Another risk inherent in POS systems is that of computer malfunction or downtime. Also, financial institutions offering POS services should provide for adequate records backup.

DEBIT AND SMART CARDS

Other funds transfer related activities that use plastic card and PIN access are debit cards and smart cards. While not EFT systems by themselves, they may be used in conjunction with EFT systems. Debit cards may draw against available balances or lines of credit in related deposit accounts. They can be used for currency withdrawals by ATMs or for the direct purchase of goods or services from retailers using POS or paper-based settlement systems.

Smart cards contain a microchip which can store customer account profiles and credit line balances, as well as a record of transactions. When the card is used to make a purchase, the amount of the purchase is deducted from the balance remaining in the card's memory. Once the credit line in the card is exhausted, it can be replenished. Smart cards do not require on-line terminals.

HOME BANKING

Home banking allows customers to determine their bank account balances, make bill payments, and transfer funds between the customer's own bank accounts via telecommunications lines. These services, which were originally performed solely by telephone, may employ either telephone or personal computers (PCs). To access the account, the customer dials a designated phone number and enters an account number and PIN. If a transfer is to be made, the customer also enters the merchants' identification numbers, customer's account number with each merchant, and the amount and date of payment. If a telephone is used, the data is called back via voice response equipment or, if by computer, the data is transmitted back to the computer terminal screen. The customer then presses a designated key to confirm the transaction. Financial institutions complete the transaction by:

- Transferring funds directly from the customers' account to the merchant accounts, if the accounts are in the same bank.
- Transferring funds into a holding account and sending a check and printout to the merchants.
- Transferring funds to the merchants' bank.
- Transferring funds to a third party who then pays the merchant or utility.

In addition to financial services, some home banking systems include programs that offer such things as:

- Stock brokerage services.
- Home information services that allow electronic access to local and regional newspapers, classified ads, and airline, restaurant, theater and sporting event reservations.

- Income tax preparation service.

INTERNAL CONTROLS FOR RETAIL EFT

Regardless of the system employed, financial institutions should ensure that adequate internal controls are in place to minimize errors, discourage fraud, and provide an adequate audit trail. Recommended internal control guidelines include:

For all systems:

- Measures to establish proper customer identification (PINs) and maintenance of their confidentiality.
- Issuance of a receipt to the customer as required by Regulation E.
- Installing a dependable file maintenance and retention system to trace transactions.
- Producing, reviewing and maintaining exception reports to provide an audit trail.
- Requiring customers of each service to sign agreements that clearly define the responsibilities of the customer and the financial institution.
- Producing and forwarding periodic customers' statements so they can review transactions made during the period and detect unauthorized transfers, as required by Regulation E.
- Confidentiality and security of customer account information including protection of PINs.
- Maintenance of contracts between bank and merchants, customer and banks, and banks and network.
- Daily reconciliation of ATM machine transactions.
- Policies and procedures regarding credit and check authorization, floor limits, override, settlement and balancing.
- Maintenance of transaction journals to provide an adequate audit trail.
- Generation and review of daily exception reports with provisions for follow-up of exception items.
- Provisions for backup and contingency planning.
- Adequate control of captured cards.
- Physical security surrounding ATM terminals.

For transfer and bill paying systems:

- Allow customers to pay bills or transfer funds only from their accounts.
- Require that all transactions be preauthorized for specifically stated customer accounts.
- Discourage payments to third parties without written authorization.

The most critical element of EFT systems is the need for undisputed identification of the customer. Particular attention should be given to the customer identification systems. The most common control is the issuance of a unique PIN that is used with a plastic card or, for non-card systems, an account number. The following guidelines, as recommended by the American Bankers Association, are encouraged.

PIN CONTROL GUIDELINES

Storage

- Unissued PINs should never be stored before issuance They should be calculated when issued and any temporary computer storage areas used in the calculation should be cleared immediately after use.
- PINs should be encrypted on all files and data bases.
- All file maintenance to PINs stored in databases should be restricted. Console logs and/or security reports should be reviewed to determine any attempts to subvert the PIN security system.

Delivery

- PINs should not appear in printed form where they can be associated with customers' account

numbers.

- Bank personnel should not be able to retrieve or display customers' PIN numbers via terminals.

- PIN mailers should be processed and delivered with the same security accorded the delivery of bank cards to cardholders. (Note: PINs should never be mailed to a customer together with the card.)

Usage

- The PIN should be entered only by the card-holder and only in an environment that deters casual entry observation.

- The PIN should never be transmitted in unencrypted form.

- PIN systems should record the number of unsuccessful PIN entries and should restrict access to a customer's account after a small number of attempts.

- If a PIN is forgotten, the customer should select a new one rather than having bank personnel retrieve the old one.

Control and security

- Systems should be designed, tested and controlled to preclude retrieval of stored PINs in any non-encrypted form.

- Application programs and other software containing formulas, algorithms, and data used to calculate PINs must be subject to the highest level of access for security purposes.

- Any data recording medium, e.g., magnetic tape and removable disks, used in the process of assigning, distributing, calculating or encrypting PINs must be cleared immediately after use.

- Employees with access to PIN information must be subject to security clearance and must be covered by an adequate surety bond. They should not be involved in card issuance operations in any way.

System design

- To limit fraud, PIN systems should be designed so that PINs can be changed without reissuance of cards.

- PINs used on interchange systems should be designed so that they can be used or changed without any modification to other participants' systems.

- Financial institutions electing to use encryption as a security technique for bank card systems are strongly encouraged to consider the Data Encryption Standards established by the National Bureau of Standards.

PLASTIC CARD CONTROL GUIDELINES

Procurement

- A written agreement between the card manufacturer and the financial institution should detail control procedures and methods of resolution to be followed if problems occur.

- Financial institutions should acquire the card manufacturer's latest third-party audit report.

- An investigation of the security devices used by the manufacturer when encoding and embossing the card should be conducted.

Embossing/Encoding

- If done by a vendor, similar precautions as detailed for card manufacturers should be considered, including written contracts and reviews of control procedures in effect.

- If done on site, the equipment should be maintained in an extremely secure area.

- Proper inventory controls over blank plastic card stock should be in place. There should be proper accounting for the number of cards used, including test cards and spoiled cards.

- Separation and rotation of duties should be practiced to the extent practical and supervisory

control reviews should be conducted on a periodic basis.

Storage

- Dual control procedures should be in place. Only a limited working supply of blank cards and cards in the process of being embossed/encoded should be allowed out of the dual custody. Adequate interim storage and accounting must exist for all cards not under dual control.

- Adequate controls should exist for captured cards.

Mailing

- Accountability controls should be created to ensure that all cards initially disbursed from the storage area are delivered to the mail area or are properly destroyed.

- Returned cards should be separately handled by a function independent of the mail department.

- Control cards should be mailed randomly to customers and their delivery validated within a few days to ensure that no theft has taken place.

TERMINAL SHARING/NETWORK SWITCHING

In an attempt to lower costs and provide widespread services, financial institutions share EFT facilities to process retail EFT services, primarily ATM and POS facilities. Some financial institutions are required by state law to share such facilities, while others voluntarily share them. EFT facilities are usually shared regionally; others voluntarily share them on a regional, nationwide and, in some cases, international basis. The most commonly shared EFT systems are:

- An EFT network formed and shared by different financial institutions.

- A multi-bank holding company network servicing affiliated banks.

- A single institution's proprietary EFT network shared with other institutions for a fee.

To facilitate use of the system, a switching network (switch) must be in place to allow shared terminals and computers to communicate with each other. The two types of switching networks used are:

- Line switching – essages are sent directly from one station to another when the central switching site establishes the connection. These systems are commonly used in real-time environments.

- Store and forward – The central switching site stores incoming messages and later retransmits the messages to their destination.

Control Requirements

The primary concerns in shared EFT facilities are security and confidentiality of customer data. These concerns become critical when the network, or any section of it, becomes inoperable or when line problems develop that interrupt the normal transfer of information through the switch. Therefore, adequate audit trails must exist for all transactions, at each switch point, identifying the originating terminal and destination.

Adequate procedures must be in place to control activity if the shared system becomes inoperable to ensure accurate posting and maintain security. Also, procedures for balancing and settling transactions should be well-documented and monitored for adherence. Each participant in the switch should receive adequate transaction journals and exception reports necessary to facilitate final settlement for their institution.

Agreements between switch or network participants must delineate each party's liabilities and responsibilities. Certain basic control items concerning normal and contingency processing must be detailed and responsibility for correction must be stated. Grievance procedures and arbitration policies should be established in order to resolve differences.

Reference is made to the Chapter 18 - Wholesale EFT for consideration of other retail EFT related concerns in the areas of input/output controls, encryption, backup, insurance, disaster recovery, and government regulations. For additional guidance also refer to the Federal Reserve's *Guide to the Federal Reserve's Payments System Risk Policy*.

This chapter is intended to determine the adequacy of controls over the retail EFT environment. The examiner must review compliance with established policy, the effectiveness of contingency/recovery planning, and assess the soundness of physical and internal controls. The reviews of work flows and control points will ensure that adequate control procedures have been established to maintain the accuracy and integrity of the data. The procedures are created, so that they may be implemented separately as part of either the IS examination or safety and soundness examinations. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

Tier I

RETAIL ELECTRONIC FUNDS TRANSFER (EFT) SYSTEMS

1. Obtain a description of each retail EFT related system operated by the institution, considering:

   a. Automated Teller Machines (ATM).
   b. Point-of-Sale (POS).
   c. Debit and/or Smart Cards.
   d. Home banking.

2. Review procedures employed for each EFT related service to ensure the integrity of plastic card and personal identification number (PIN) processing, including separation of functions over issuance of the cards, issuance of PINs, storage of cards and maintenance of software controlling PINs. The review should focus on controls that could lead to widespread misuse and significant losses to the institution.

3. Review a sample of agreements for each EFT related service to ensure that they adequately set forth responsibilities and liabilities of the institution and the customer, primarily as to requirements of the Electronics Funds Transfer Act (Regulation E).

4. Determine that a viable and tested contingency plan is in effect. The plan should provide for short-term recovery of data in-process, security, confidentiality of customer data, and reasonable time frames for full recovery, in relation to the volume and importance of the application to the institution's operation.

5. If applicable, review agreements with other switch or network operators to ensure each party's liabilities and

responsibilities are clearly defined, especially in the areas of settlement, security and confidentiality, and contingency processing.

6. Compare the last executed internal audit procedures covering each EFT related operation to the related questions detailed in Tier II of these procedures, and determine whether they meet or exceed Tier II coverage.

7. Determine that the audit function periodically performs an inventory of all EFT stations owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).

8. Review all audit reports covering any EFT related operation determine the current status of any exceptions noted in the audit report.

9. Procedures included in Tier II that are not sufficiently covered under steps 6 and 7, must be implemented in this examination. (Note: To the extent coverage is clearly satisfactory and current, audit procedures and workpapers may also be utilized to address steps 2 through 5).

CONCLUSIONS

10. Review the results of work performed in this chapter and in the chapters for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

11. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

12. Assign rating, (see Chapter 5 for additional information).

13. Prepare an index of workpapers for this section of the workprogram.

14. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

15. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

(Note: Includes automated teller machines (ATM), point of sale (POS), debit/smart cards and home banking. To the extent the operations are autonomous, applicable questions should be applied separately for each application.)

ACCOUNTING AND PROCESSING

1. Are all general ledger accounts related to retail EFT reconciled on a timely basis?

2. Is each EFT system and origination site reconciled daily and are reconciling items adequately controlled?

3. Are reconcilements and exception items regularly reviewed by supervisory personnel?

4. If the institution is a participant in any shared EFT networks, is daily settlement with each network current and are reconciling items adequately controlled?

5. Are separate accounts used to control adjustments, unposted items, rejects, etc. and are they periodically reconciled?

6. For input reconstruction, are transactions files duplicated or otherwise retained for a minimum of 60 days as required by Regulation E to identify unauthorized transactions?

7. Is a separate investigation unit in place to control customer inquiries, unposted items, rejects, differences, etc., and do they periodically generate reports of outstanding items and aging for management?

8. Are exception reports (e.g., unposted items, rejects, differences, and aging of open items) receiving appropriate attention?

9. Is separation of duties maintained throughout each Retail EFT accounting process including receipt of transactions, file updates, adjustments, internal reconcilement, preparation of general ledger entries, posting to customers accounts, investigations, and reconcilement with network processors?

10. Are adjustments (e.g., changes to deposits and reversals) to original retail EFT instructions received by an individual that does not have access to the data or customer files?

PERSONAL IDENTIFICATION NUMBERS (PIN)

11. Is access to PIN data and operations completely removed from functions preparing or issuing plastic cards?

12. Are new PINs entered into the system by personnel who do not open accounts or have access to customer account information?

13. If issuance of a new PIN is necessary, have control procedures been established and is there accountability to the individual initiating such a transaction?

14. Are PINs issued in an environment that precludes matching them to customer account numbers or access forms (e.g., plastics)?

15. Is access to a customers account restricted after a small series (e.g., three) unsuccessful attempts to enter the correct PIN?

16. Are PINs encrypted or otherwise disguised when stored on computer files or transmitted over telecommunications lines?

17. Do procedures prohibit PIN information from being released via telephone?

18. If access to PINs maintained on computer files must be accessed for maintenance purposes, are activities closely supervised and is each occasion logged?

19. When selecting PINs, are customers discouraged from using common words or sequences numbers and words or numbers that can easily identify the customer?

PLASTIC CARDS

20. Are all retail payment cards:

    a. Issued only as required?

    b. Kept in a locked, secure location under dual-control?

    c. Controlled by access logs?

    d. Periodically inventoried?

21. Are blank cards kept under effective dual control and accounted for in each of the various steps in encoding, embossing and mailing?

22. Is access to the physical area in which encoding is performed restricted from access by unauthorized personnel?

23. Is the working supply of plastics stored in a secure environment?

24. Is use of encoding equipment well controlled?

25. If cards are issued at more than one location (e.g., branches), have accountability and card control procedures been established for each location?

26. Are cards mailed to customers in envelopes with a return address that does not identify the institution?

27. Are returned cards controlled and accounted for by individuals who do not issue cards or have systems/operations responsibilities?

28. Is it against policy for the institution to mail unsolicited cards?

29. Are cards which were captured or inadvertently left at EFT terminal locations properly controlled?

30. Are plastic cards and PINs always mailed separately and with a sufficient period of time between mailings?

31. After a card is issued, is there follow-up to ascertain whether both card and PIN were received/utilized by the proper customer?

32. Are procedures such as hot card lists and expiration dates used to limit the period of exposure if a card is lost, stolen or purposely misused?

33. Are spoiled cards destroyed under dual control and are records maintained of all destroyed cards?

34. Are test or demonstration cards adequately controlled?

35. Are satisfactory controls maintained over any duplicate cards which were not issued to the customer (e.g., temporary access)?

36. If vendors are employed to produce cards, have reviews been conducted by the institution or for the institution (e.g., third party or cooperatively with other users of the vendor) that meet or exceed the measures noted under PINs and Plastic Cards, above, as applicable?

OPERATIONAL CONTROLS

37. Are ATM data entry personnel prohibited from originating entries for processing or physically handling cash?

38. Is proper control of source documents (e.g. checks for deposit) maintained throughout the daily processing cycle relative to the following aspects:

    a. Input preparation?

    b. Reconcilement of item counts and totals?

    c. Output distribution?

    d. Storage of the instruments?

39. Are terminal and operator identification codes used for all types of retail EFT transactions?

40. Does the system prevent customer charges from exceeding the available balance in the account and/or approved overdraft lines?

41. Are access to and use of terminals used to change customer credit lines and account information adequately controlled?

42. Are retail EFT equipment keyboards and/or display units properly shielded to avoid disclosure of customers IDs or PINs?

43. Do customers receive a receipt showing the amount, date, time and location for retail EFT transactions?

44. Is each retail EFT transaction assigned a sequence number and terminal ID to provide an audit trail?

45. Are hot card or customer suspect lists regularly updated and distributed to each user location?

46. Is each home banking customer required to pre-authorize payments to specific merchants and/or transfers between accounts?

47. Are verification procedures in place for telephone instructed payments or transfers and are confirmations promptly sent to customers and merchants?

48. Are security devices and procedures for each EFT facility adequate?

49. Are merchants prohibited from accessing customer accounts or account information?

50. Are tests of program changes to retail EFT applications adequately controlled and are logs maintained for each test showing purpose and results?

51. Are software and equipment maintenance personnel closely supervised and are their activities logged?

AGREEMENTS/CONTRACTS

52. If the institution is a participant in any shared EFT network, do the written agreements between/among participants and operators of the network clearly set forth the rights and responsibilities of all parties, including security and confidentiality of customer information, settlement terms, contingency operations, and requirements for installing and servicing equipment and software?

53. Are agreements in effect with all vendors supplying services for retail EFT operations (e.g., plastic cards, equipment/software maintenance or ATM cash replenishment) that clearly define the responsibilities of both the vendor and the institution and do they provide for minimum control standards, the ability of the institution to audit the vendors operations, periodic submission of financial statements to the institution and contingency plans?

54. Are agreements in effect with all customers for each retail EFT service provided by the institution and do the agreements set forth the responsibilities and limits of liability of both the customer and the institution and do they include provisions of the Electronic Funds Transfer Act (FRB Regulation E) and the Expedited Funds Availability Act (FRB Regulation CC) for deposit activities?

CONTINGENCY PLANS

55. Have written contingency plans been developed and tested for partial or complete failure of each retail EFT system and/or communication lines between the institution, networks, and data center? Are the plans reasonably comprehensive in relation to the volume and importance of the specific Retail EFT activity to the institution's operation? At a minimum, do they provide for satisfactory store and forward procedures to protect against loss or duplication of data and for full recovery within a reasonable time period?

OTHER

56. Is there an internal control risk assessment (per FDICIA 112)? Assess its adequacy.

57. Is each individual site providing retail EFT services periodically reviewed by management to ensure policies and procedures, security measures, and equipment maintenance requirements are being adhered to?

58. If vendors are employed to perform any major services related to Retail EFT activities, are annual financial statements received and reviewed; and are reports covering audits of the vendors periodically obtained and reviewed?

59. Proceed to step 10, Tier 1.

Examiner | Date

_____|_____

Reviewer's Initials

AUTOMATED CLEARING HOUSE (ACH) CHAPTER 21

(FILE NAME ON DISK #2 = S2C21.WPD)

The ACH payments mechanism was developed in the early 1970s as an electronic substitute for paper based payments. Today, the ACH is a nationwide electronic payments system used by a large number of depository institutions and corporations. ACH rules and regulations are established by the National Automated Clearing House Association (NACHA) and the local ACH associations, and are incorporated by reference in the Federal Reserve Bank's ACH operating circulars.

ACH is a value-dated system that supports both credit and debit transactions. In ACH credit transactions, funds flow from the depository institution originating the transaction to the institutions receiving the transactions. Examples of credit payments include direct deposit of payroll, dividend and interest payments, Social Security payments, and corporate payments to contractors and vendors. In a debit transaction, funds flow from the depository institution receiving the transaction to the institution originating the transaction. Examples of ACH debit transactions include collection of insurance premiums, mortgage and loan payments, consumer bill payments, and corporate cash concentration transactions. ACH transactions are deposited in batches at Federal Reserve Banks (or private-sector ACH operators) for processing one or two business days before the settlement date. These transactions are processed and delivered to the receiving institutions through the night processing cycle for a given day.

GROWTH

Over the last seven years the volume and dollar value of ACH credit transactions have increased 23 percent and 30 percent per year, respectively. Additional uses of the ACH, such as bill paying services, continue to be developed as depository institutions, corporations, and consumers realize its efficiency and low cost compared to large dollar payments systems and check payments. Another area of growth is the use of debit transactions for the collection of large payments due the originator, such as cash concentration of a company's nationwide branch or subsidiary accounts into one central account and other contractual payments of a recurring nature.

OPERATORS

The Federal Reserve is the principal ACH operator. In addition, there are several private sector ACH operators including the New York Automated Clearing House Association (NYACH), VISA, and the Arizona Automated Clearing House Association (ACHA). VISA and ACHA use the Federal Reserve to process transactions which are delivered to depository institutions that are not members of VISA or ACHA. NYACH serves as the ACH processor in the Second Federal Reserve District and uses the Federal Reserve Bank of New York as a communications facility for interregional transactions originated and received by NYACH members.

For the Federal Reserve ACH system, depository institutions send ACH transactions to and receive ACH transactions from the Federal Reserve by direct computer interface connection or by personal computer connection. Third-party processors also may send ACH files to a Reserve Bank on behalf of a depository institution.

RISKS AND EXAMINATION CONCERNS

As with any funds transfer system, there are inherent risks in using the ACH, including error, credit risk and fraud. When reviewing ACH activities, examiners should evaluate the following:

- Agreements maintained by the depository institution as an originator and/or receiver of ACH transactions covering delivery and settlement arrangements.
- Balancing procedures for ACH transactions sent to and/or received from an ACH operator.
- Monitoring of institution's and customers' intraday and interday positions.

- The credit policy and effectiveness of procedures to control intraday and overnight overdrafts, resulting from extensions of credit to ACH customers, to cover the value of credit transfers originated. (Note: Since the ACH is a value-dated mechanism and transactions may be originated one or two days before the settlement date, the originating institution is exposed to risk from the time it submits ACH credit transfers to the ACH processor until the time its customer funds those transfers.)

- Credit assessments of customers originating large dollar volumes of ACH credit transactions. Ensure that these credit assessments are reviewed periodically to ensure that recent economic conditions having a possible impact on customers' financial position are taken into consideration.

- Uncollected funds controls and related credit policy for deposits created through ACH debit transactions. (Note: Although the Federal Reserve makes funds available on the settlement date, these are provisional funds because ACH debits may be returned for insufficient funds or other reasons (e.g., court order)).
- Exception reports, i.e., large item and new account reports.

- Control procedures for terminals through which additions, deletions, and other forms of maintenance could be made to customer databases.

- The retention of all entries, return entries, and adjustment entries transmitted to and received from the ACH for a period of six years after the date of the transmittal. (This is a NACHA requitement.)

Reference should also be made to Chapter 18, Wholesale EFT for additional consideration of ACH related concerns in the areas of input/output controls, encryption, backup, insurance, and disaster recovery. For additional guidance also refer to the Federal Reserve's *Guide to the Federal Reserve's Payments System Risk Policy*.

This section is intended to determine the adequacy of controls over the ACH environment. The examiner must review compliance with established policy, the effectiveness of contingency/recovery planning and assess the soundness of physical and internal controls. The reviews of work flows and control points will ensure that adequate control procedures have been established to maintain the accuracy and integrity of the data. The procedures are created so that they may be implemented separately as part of either the IS or safety and soundness examinations. The examiner should document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

Tier I

AUTOMATED CLEARING HOUSE (ACH)

1. Determine the nature and characteristics of the system/network in use by:

   a. Identifying the source of ACH activities.

   b. Determining whether customers are performing their own input or the financial institution is using third party servicers or multiple ACH operators.

   c. Identifying both the hardware and software being used in-house to support these ACH activities.

2. Review policies and procedures in place to monitor customer balances for credit payments (e.g., payrolls) to ensure that payments are made against collected funds or established credit limits, and that payments in excess of established credit limits are properly authorized.

3. Determine if deposits resulting from ACH transmitted debits on other accounts are treated as uncollected funds until the institution has reasonable assurance that the debits have been paid by the institution on which they were drawn. Also, if drawings against uncollected funds are monitored to ensure they are within established guidelines.

4. Review a sample of contracts authorizing the institution to perform ACH activities for customers to determine if they adequately set forth responsibilities of the institution and the customer, primarily as they relate to the following rules established by NACHA:

a. Is the institution operating within established ACH operating rules and regulations?

b. Are agreements in effect for all ACH customers (incoming and outgoing) that set forth the responsibilities of the institution and customers and do the agreements include the rules of the ACH; funding arrangements (outgoing); Expedited Funds Availability Act (FRB Reg. CC); and UCC4A (credit transfer only)?

5. Have ACH activities been considered in the institution's overall insurance program?

6. If third-party processors are employed to perform any major services related to ACH activities, are annual financial statements received and reviewed; and are reports covering audits of the processors periodically obtained and reviewed?

7. Compare the last executed internal audit procedures covering ACH operations to the related questions detailed in Tier II of these procedures, and determine whether they meet or exceed Tier II coverage.

8. Review a sufficient sample of supporting audit workpapers necessary to confirm that they support the execution of procedures established in step 7.

9. Review all audit reports related to the ACH and determine the current status of any exceptions noted in the audit report.

10. Procedures included in Tier II that are not sufficiently covered under steps 7 and 8, are to be implemented as part of this examination. (Note: To the extent coverage is clearly satisfactory and current, audit procedures and workpapers also may be used to address steps 1 to 4.)

CONCLUSIONS

11. Review the results of work performed in this chapter and in the chapters for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers

should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

12. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

13. Assign rating. (see Chapter 5 for additional information.)

14. Prepare an index of workpapers for this section of the workprogram.

15. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

16. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

ACCOUNTING AND PROCESSING

1. Is a log maintained of the ACH payments received from and delivered to each customer?

   a. Are all payments received, balanced to the aggregate of payments sent to an ACH operator?

   b. Are all payments received from an ACH operator balanced to the aggregate of payments delivered to customers?

2. Are all general ledger accounts related to ACH reconciled on a timely basis?

3. Are reconcilements and exception items regularly reviewed by supervisory personnel?

4. Are daily activity and pending files with the ACH operator reconciled daily?

5. If applicable, is activity with third-party processors preparing ACH transaction files reconciled daily?

6. Are holdover transactions adequately controlled?

7. Are individual outgoing batches reconciled before being merged with other ACH transactions?

8. Are separate accounts used to control holdovers, adjustments, return items, rejects, etc. and are they periodically reconciled?

9. Is a separate investigation unit in place to control customer inquiries, return items, rejected/unposted items, differences, etc., and do they periodically generate reports of outstanding items and aging for management?

10. Does management adequately track exceptions to credit limit policies and legal contracts?

11. Are exception reports (e.g., rejects, return items, and aging of open items) receiving appropriate attention?

12. Is an adequate separation of duties maintained throughout the ACH process including origination, data entry, adjustments, internal reconcilement, preparation of general ledger entries, posting to

customers accounts, investigations, and reconcilement with ACH operators?

13. Are reference manuals available to data entry personnel? Do manuals address:

    a. Credit relationships?

    b. Internal control policies and procedures?

    c. Operational procedures and controls?

    d. Data security/customer security issues?

14. Are adjustments (e.g., added payments, stop payments, reroutes, and reversals) to original ACH instructions received in an area that does not have access to the data files?

15. Are assurances made that the individual making the request for an adjustment is authorized (e.g., signature verification and call backs on telephone instructions) and are records maintained (e.g., logs and taping of telephone calls) of individuals making the request?

16. Is it required that master customer profile originations and change requests:

    a. Are in writing?

    b. Identify the originating personnel?

    c. Document supervisory approval?

FUNDING AND CREDIT

17. Before releasing payments to an ACH operator, are assurances obtained that sufficient collected funds (e.g., on deposit or prefunded) or credit facilities are available?

18. If prefunding arrangements are in place for customers without credit lines, are funds either blocked (held for disposition) or maintained in separate accounts until the transaction date?

19. If not prefunded, are blocks placed for outgoing payments on deposit accounts; applied as reductions to credit lines; or included in the overall funds transfer monitoring process?

20. Are payments resulting in extensions of credit lines or drawings against uncollected funds properly approved, and is documentation maintained to support the approvals?

21. If third-party processors are employed to process outgoing ACH transactions, are procedures in place to monitor ACH activity and ensure that funds are collected (collected balances, prefunding, credit lines) before the institution settles with the ACH operator?

22. Are ACH debits deposited treated as uncollected funds and are drawings against such funds adequately monitored for debits originated by high-risk customers?

23. Are drawings against uncollected ACH deposits properly approved, and is documentation maintained to support approvals for debits originated by high-risk customers?

24. Is there an internal control risk assessment (per FDICIA 112)?

25. Does management perform a risk assessment of the area in terms of the importance of the function to the overall corporate services function?

SECURITY

26. Is a comprehensive data security system maintained that provides segregation of duties performed via computer terminals, such as data entry, adjustments, and release to the ACH operator?

27. Does the maintenance of the security systems include periodic changes of passwords, protection of password files, non-display of passwords on terminals, and automatic shut-down of terminals not in use?

28. Is data pending release to the ACH operator maintained in an environment that protects the data from unauthorized change?

29. Are telecommunications lines used to receive data from customers and to transmit data to ACH operators encrypted?

30. Are magnetic tapes and/or other data (computer or manual listings) submitted by customers protected from unauthorized access from the time they are

received by the institution until they are entered into the ACH system?

31. Is adequate physical security maintained over ACH operating areas?

CONTINGENCY

32. Has a written contingency plan been developed and tested for partial or complete failure of the system and/or communication lines between the institution, ACH processor, customers, and data center? Is the plan reasonably comprehensive in relation to the volume and importance of ACH activity to the institutions operation? Do the procedures provide for a reasonable recovery period?

33. For input reconstruction, are transactions files duplicated or otherwise retained for a minimum of 24 hours?

34. Determine if data and program files are adequately retained and backed up at off-premises facilities.

35. Determine if the center has established and tested procedures to recover and restore data.

36. Determine if the frequency and methods of testing contingency plans are adequate.

37. Proceed to procedure 11, Tier 1.

Examiner | Date

_____|_____

Reviewer's Initials

IS SERVICING – PROVIDER AND RECEIVER

CHAPTER 22

(FILE NAME ON DISK # 2 = S2C22.WPD)

Information Systems (IS) servicing can be viewed from the perspective, of the service provider or the receiver. Many control and administration issues are common to both. Although control issues are usually discussed from the viewpoint of the service provider, most are also pertinent to the service receiver. Separate workprograms have been provided in this chapter to aid examiners in reviewing servicing activities from the two distinct perspectives.

IS controls are important in the customer servicing and user control areas. Controls similar to those in other information processing areas should be used in customer servicing and user operations to maintain information integrity. This is particularly important when IS servicing is performed off-site.

The interchange of services between organizations entails certain risks and responsibilities that must be addressed by both the servicer and the user. Some of these can be defined and delegated within a service contract; others must be handled by each party through implementing proper operational controls.

This section describes operational and technological controls, guidelines for insurance coverage, and servicing contracts. Also discussed are adverse servicing contracts and improper financial inducements to insured financial institutions. This chapter addresses the responsibility to obtain and analyze adequate financial information from the servicer and/or client. Financial institutions depend increasingly upon servicers to provide information processing. The most difficult operational calamity for a financial institution to provide for is the termination of processing services from the servicer's bankruptcy. This chapter discusses issues specifically affecting service providers and examination objectives for reviews of service receivers.

Under provisions of the Bank Service Corporation Act, Sec. 1867, when a financial institution contracts for information processing services, it must notify its primary regulatory agency of this service relationship. The institution should notify its agency within 30 days after signing a contract or the commencement of services, whichever occurs first.

USER INSTITUTION CONTROLS

When IS services are provided by an external servicer, many of the financial institution's operational controls should be extended to encompass the servicer. Using computerized programs and networks, financial institution employees maintain millions of accounts and record similarly high numbers of transactions every day. Text processing systems store vast amounts of correspondence. Financial institutions routinely transfer their own and customer funds ranging in the billions via computerized systems.

Transmission of data and funds regularly occurs over public communications links, such as telephone lines and via satellite. The use of new technologies to transfer funds and records, while improving customer service and institutions' internal operations, also has increased the chances of errors and abuses, such as loss of funds, loss of competitive advantage, lawsuits arising from damaged reputations, improper disclosure of information, and regulatory sanctions.

Controls must be created to minimize the vulnerability of all information and to keep funds secure. Management must assess the level of control against the degree of exposure and the impact of unexpected losses on the institution. Various ways are available to strengthen information and financial security in financial institutions. The most basic are sound policies, practices, or procedures, including physical security, separation of duties, internal quality control, hardware and software access controls, and audits.

Management should institute information security controls 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 damage or destruction of information.

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.

In many cases, financial institutions have chosen to establish and communicate security principles in writing. If sound principles are not effectively practiced, the regulatory agency may require management to establish written policies to formally communicate risk parameters and controls.

Examiners may periodically conduct reviews of information security. These reviews may include:

- The adequacy of security practices.
- Compliance with security standards.
- Management supervision of information security activities.

Manual Controls

The following discussion briefly covers basic operational controls that should be in place in a serviced institution environment. Similar controls also apply to work processed by a separate IS department within the user's own institution.

Separation of Duties

A basic control used in any internal control system is separation of duties. With this control in place, there must be collusion for any improper activities to occur. Therefore, no one person should be able to initially authorize and execute a complete transaction. Servicer personnel should not initiate transactions or correct data except when such activity is required to complete processing in a reasonable time period. If this unusual situation arises, transactions should be approved by appropriate levels of management at the information processing center and at the serviced institution. Documented approvals, with details of the circumstances that required this action, should be maintained at the processing center and the serviced institution.

Input and output duties normally should not be performed by the same person. In some instances, staff limitations may cause one person to be responsible for several activities. Included among these concentrated activities are:

- Preparing data for input to the system or shipment to the external servicer.
- Performing data entry functions, including operating check reader/sorter machines, proof machines or data conversion devices such as optical scanners or other imaging equipment.
- Preparing rejects for reentry into the system; reconciling output to input or balancing the system.
- Distributing output to ultimate users.
- Posting the general ledger and balancing computer output to the general ledger.

Internal control may be improved through rotation of assignments and scheduled, periodic absences. This will help prevent one person from having total control over any one job for an extended time period and will provide cross-training and personnel backup. These absences are most effective if they extend over the end of an accounting period or for two or more consecutive weeks.

Written policies and procedures, when used as training and reference documents, may help facilitate job rotation. Application manuals usually consist of a user's guide provided by the servicer and supplemented by procedures written by the user. Manuals normally cover preparation and control of source documents, and certain control practices pertaining to moving documents or electronic images to and from the user and servicer, the daily reconcilement of totals to general ledger, and changes to master files.

Dual control should be used in automated systems. Supervisory holds should be placed on customer accounts that require special attention. Certain types of transactions, e.g., master file changes, should require special transaction codes before the activity can be completed. When account information is added/removed or when a transaction requiring supervisory approval is completed, exception reports will be printed and should be promptly reviewed by a designated person not involved with the original transaction. In general, automated dual control methods are superior to manual procedures. Many current financial software applications use automated balance and control features. Presentations to the users are performed on-line rather than using a manual comparison of hardcopy reports to source documents.

Internal Quality Controls

Internal controls fall into three general categories: administrative, dollar, and nondollar.

Administrative controls usually result from management review of daily operations and output reports. Each application includes basic controls and exception reports that are common to all financial institution operations. To be effective, exception reports and controls must be properly used, especially methods for controlling dormant accounts, kiting, drawings against uncollected funds, overdrafts and posting computer-generated income and expense entries.

Dollar controls ensure processing for all authorized transactions. Balancing procedures should be complete and trial balances must be reconciled to original source input and to the general ledger. Report distribution should follow a formal procedure. All rejects must be accounted for, corrected and resubmitted, and all exception reports should receive proper supervisory attention.

Nondollar control totals are used when dollar values are not present, as in name and address changes. Controls should be established before processing this work and be properly reviewed to ensure that all nondollar transactions are being processed. For example, new account reports should be checked against new account input forms or written customer account applications to assure that data has been properly entered. To protect data integrity, procedures should be developed to control master file and program changes. The serviced institution should verify that only its authorized changes are used to alter information, and that the processing center employees do not initiate master file changes.

TECHNOLOGY CONTROLS

Data Communications

Data communications system controls should be reviewed by the serviced financial institution. The controls available to the user can be generally categorized into: user identification, levels of accessibility, restricted transactions, and activity and exception reports.

User Identification

This control allows only authorized personnel to use the system and requires personal and workstation identification for each transaction entered. Users may be identified by key, token, password and/or identification number (IDs). When workstations are equipped with key, card-type locks, or tokens, strict control of access devices is necessary to protect the computer system. Many systems use software controls which require passwords and/or IDs to gain access to the system. Security procedures should strictly control access to those user IDs, and passwords/numbers should be changed regularly. Some workstations can be controlled by restricting access to the work area by placing them in a remote or locked area, or by establishing definite times for remote activity via system invoked time-of-day controls. Servicers may offer these features as standard access control elements, but actual information security practices could vary widely at

the serviced institution level. Therefore, it remains important to determine that these controls are implemented properly by the serviced institution.

When a workstation is not hardwired or permanently connected to a host computer, special manual and automated controls must be established to ensure proper host/terminal relationships. Automated dial-back procedures may be used, where the computer calls the PC back to authenticate access. Other automated methods may include software checks on hardwired terminal ID numbers, or a dialogue between the data communications software and workstation or PC.

Level of Accessibility

Another basic control is to allow each user to access only that information needed for that person's duties. One person should not be able to make all transactions relating to a given event. For example, when a loan is charged-off, one person should not control adjustments to both the loan and general ledger applications without appropriate compensating controls. In those systems where the general ledger entries are auto-posted, another staff member should review the general ledger entries promptly.

An automatic timeout feature provides a benefit with minimal processing risk. Since the unattended workstation can be a target for unauthorized use, this feature guards against this by automatically signing-off a user from a workstation where there has been no activity for a certain period of time. There is little user inconvenience in this feature, since to restart, the user need only reenter a password. Using time-of-day restrictions can limit unauthorized use of workstations during periods when the entire department or section would be unattended.

Restricted Transactions

Restricted transactions are specialized transactions used only by supervisory or management personnel. Examples are reversing transactions, dollar adjustments to customer accounts, or daily balancing transactions. Management should review periodically user needs and the appropriateness of restricting access to these transactions.

Activity and Exception Reports

Report output will vary depending on the sophistication of data communications and applications software. At a minimum, reports should be generated that detail transactions by workstation, operator and type. More sophisticated software will produce such reports as the number of inquiries by workstation, unsuccessful attempts to access the system, unauthorized use of restricted information, and any unusual activity, Eg., infrequently used transactions.

Activity reports monitor system usage and should be reviewed periodically by management. Exception reports should be produced and reviewed daily by designated personnel who have no conflicting responsibilities. A problem with many logging systems is that every event is recorded in the log and therefore identifying problem areas is, in many instances, cumbersome and difficult. Some operating system vendors or third-party software companies can provide software that produces more meaningful analysis and reporting from these logging systems.

Systems Features and Controls

As a communications system becomes more sophisticated, the controls also will become more complex. Generally, communication systems fall into basic levels: inquiry only, memo-post, and on-line post. However, a number of combinations and variations of these levels of systems exist and are described as follows:

- *Inquiry-only system.* This system gives the user the ability to search and review machine-readable records, but not to alter them. The number of controls and security concerns related to this system are few. A major concern is the access to confidential information.

- *Memo-post system.* This level is more sophisticated than the inquiry-only system and allows the user to create interim records. Permanent posting is done by the servicer through batch processing. Memo-post systems should be controlled by limiting physical and logical access to the system and restricting certain transactions to supervisory personnel only.

- *On-line post system.* This system, sometimes called a real-time system, requires the strictest controls because all accepted transactions entered through the communications system are permanently applied to the machine-readable records. Besides controlling access, the reports produced by the system should provide all activity and exception information and should be reviewed by appropriate levels of management.

Backup Considerations

Data communications systems are susceptible to software, hardware, and transmission problems that may make them unusable for extended periods of time. If the financial institution depends on its data communication system for its daily operations, appropriate backup provisions are necessary. Backup is the ability to continue processing applications in the event the data communication system fails. Backup can be provided in a number of ways, including via a batch processing system or PCs operating in an off-line mode, data capture at the controller if transmission lines are lost, redundant data communication lines, backup modems, or rerouted circuits from the local telephone carrier.

Regardless of the method used, a comprehensive backup plan with detailed procedures is required. Detailed procedures on how to obtain and use personnel and equipment must be included in the plan. Because of the critical nature of some on-line systems, a batch backup may not remain a viable option. Periodic tests of backup capabilities should be performed to ensure that protection is available and that employees are familiar with the plan.

Other Operational Controls

Audit

The reliability of the audit review of work processed by the servicer must be determined. Therefore, the audit review should consider the following factors:

- The practicality of the serviced institution having an internal auditor and if so, the auditor's level of training and experience.
- The training and background of the serviced institution's external auditors.
- Audit functions performed by the institution's outside auditors, by the servicer, by the servicer's outside auditor and by supervisory personnel.
- Internal IS audit techniques currently followed.

The audit should review controls and operating procedures that help protect the institution from losses due to irregularities and willful manipulations. Thus, a regular, comprehensive audit is necessary.

CPA audit reports generated on external IS servicers typically recite certain internal control measures that client institutions are responsible for, and that they must have in place in order for the servicer's accounting systems to be effective. These client institution internal control measures are essential. Financial institution management and their audit personnel should verify that the recommended institution internal controls are working effectively at their own organization, and that they effectively complement the accounting system controls described in the servicer's third-party review (See Chapter 1 for additional information on types of external audit reports and their scope).

Because of the need for an effective internal control network at the serviced institution, around-the-computer audit techniques should be performed periodically by designated personnel:

- Developing data controls (proof totals, batch totals, document counts, number of accounts, and pre-numbered documents) at the institution before submission to the servicer. The auditor should sample the controls periodically to ensure their accuracy.
- Spot-checking reconcilement procedures to ensure output totals agree with input totals, less any rejects.
- Sampling rejected, un-postable, holdover, and suspense items to determine why they are unprocessable and how they are disposed of (to assure they are properly corrected and reentered

on a timely basis).

- Verifying selected master file information (such as service charge codes), reviewing exception reports and cross-checking loan extensions and deposit account entries to source documents.

- Spot-checking computer calculations, such as loan rebates, interest on deposits, late charges, service charges, and past-due loans.

- Tracing transactions to final disposition to ensure there are adequate audit trails.

- Reviewing source input to ensure that sensitive master file change requests have the required supervisory approval.

- Visiting the servicer periodically to assess the status of controls.

- Examining other audits of the servicer.

In addition, through-the-computer audit techniques allow the auditor to use the computer to check processing steps. There are audit software programs to test extensions and footings, and to prepare direct verification statements. These audit software programs often can invoke statistical sampling routines in generating their audit confirmations. If a serviced institution has audit software, provisions should be made with the servicer to allow its use.

Regardless of whether the information processing is done internally or through an outside servicer, the financial institution's board of directors must provide an adequate audit program for all information systems. If the institution has no internal IS audit expertise, the nontechnical audit methods can provide minimum coverage. This should be supplemented by comprehensive outside IS audits (See Chapter 1 for additional information on types of external audits, their reports, and their scope).

INSURANCE FOR USER INSTITUTIONS AND SERVICER PROVIDERS

A financial institution should review its internal operations, the transmission or transportation of automated records or data, and the type of processing being performed at the servicer. This review should identify the risks and accountability at both, the user and servicer locations, and while in transit. The institution should review the available insurance coverage to determine what coverage should be obtained by the institution (See Chapter 9: Management for additional information on insurance coverage). Insurance covering physical disasters, such as fire and natural disasters, should be sufficient to cover replacement of the computer system. Coverage that protects specialized computer and communications equipment may be more desirable than that provided by regular hazard insurance. Expanded coverage provides protection against water infiltration, mechanical breakdown, electrical disturbances, excessive changes in temperature, corrosion, etc. The use of an agreed-amount endorsement can provide full recovery of covered loss.

Coverage in effect at the servicer should be reviewed to determine if its amounts and types are adequate and that it is the same as the financial institution would purchase if the processing was done internally. Coverage provided by the servicer should complement and supplement the institution's coverage. Where servicer coverage is not sufficient, the user institution should consider obtaining coverage. Additionally, if the loss is under the user's coverage, it need only prove that a loss occurred to make a claim. If the loss is under the servicer's coverage, the institution must prove that it occurred and was caused by the servicer, in order to make a claim. The serviced institution's blanket bond coverage should be reviewed, as well as, similar coverage provided by the servicer. Standard Form 24 fidelity coverage (also called the Financial Institution Bond) provides the institution with broad risk coverage.

The coverage period is stated in terms of a fixed time period. The loss, the discovery, and the reporting of the loss to the insurer must occur during that stated period. Extended discovery periods are available generally at additional cost if the bond is not renewed. The dollar amount of the coverage now represents an aggregate for the stated period. Each claim paid, including the loss, court costs, and legal fees, reduces the outstanding amount of coverage, and recoveries do not reinstate previous levels of coverage. The serviced institution's board of directors should be involved in determining insurance coverage, because each board member will acknowledge the terms, conditions, fees, riders,

exclusions, etc., of the policy. The institution must report to the insurer any existing regulatory examination findings, memorandum of understanding, cease and desist order, etc. Information provided to the insurer is considered a warranty of coverage. Any omission of substantive information could result in coverage being voided.

The institution or servicer should consider additional coverage for:

- Media reconstruction to recover the data contained on the magnetic media.
- Media replacement to replace blank media.
- Extra expense to provide reimbursement of expenses incurred over the normal cost of operations.
- Business interruption and errors and omissions coverage by the servicer.
- Transit coverage for physical shipment of source documents.
- EFTS liability coverage for operations which use electronic transmission.
- Computer systems rider to the financial institution bond which provides coverage for employee dishonesty involving the institution's computer and wire transfer systems.
- Computer crime policy which provides broader coverage than the computers systems rider, and when sold with the financial institution bond, replaces the computer systems rider. The computer crime policy affords protection against both internal and external perpetrators of computer crime and damage done by computer viruses and hackers.

The determination of purchase insurance coverage or to self insure is based on several factors: The cost of coverage versus the probability of occurrence of a loss; the cost of coverage versus the size of the loss of each occurrence; and the cost of coverage versus the cost of correcting a situation which could result in a loss. In order to evaluate these risks and the costs of insuring against these risks, some institutions engage risk consultants. In situations where the risks are complex or the expertise of management is limited, the analysis of the proper types and amounts of insurance protection needed may best be performed by outside experts. Certain criteria should be used when using a consultant for this review: The consultant should not be affiliated with an insurance company; should not currently be underwriting or selling insurance to the financial institution; and should have a good reputation in the marketplace.

RECORD PROTECTION AND RETENTION FOR USER INSTITUTIONS

The ability of any financial institution's IS operations, whether performed internally or by an outside servicer, to survive a disaster, depends on the retention of sufficient backup data to reconstruct the institution's important records and sufficient backup capacity to process them.

When the institution is serviced, records are controlled by both the servicer and the institution. In order to provide sufficient coverage, a determination should be made as to which records are best protected at the servicer and which are best protected by the institution. The servicer's responsibility for records it stores for the institution should be detailed in the service contract. If the servicer does not, or will not, permit specific reference to record retention in the contract, then a general reference may be sufficient if closely reviewed by the institution. The institution should obtain a copy of the servicer's backup agreement and retention procedures and thoroughly understand what records are protected and to what extent. The institution should keep on file the servicer's procedures and review them periodically.

In addition to records retention procedures, the institution should review the servicer's hardware and software backup arrangements. The review should encompass the frequency of data and software backups, the location of the off-site storage facility and the materials stored at that site, the availability of software replacement or vendor support, and the amount and location of duplicate software documentation.

The servicer's hardware backup arrangements should be reviewed to determine: (1) if a commercial

recovery service is used and the amount and type of backup capacity provided under the contract; (2) if the servicer uses an alternate data center, and if the center has sufficient capacity and time to allow continued full service; or (3) if multiple processing sites within the same facility are available for non-disaster processing problems, and whether each site has an alternate or uninterruptible power supply. Arrangements at an alternate site should be able to provide adequate communications, continued transmission of data, and preparation of reports.

Some servicers do not automatically provide recovery services in normal processing agreements. Management must be sure they are covered for recovery services. Examiners should determine if a recovery service has been subscribed to or another means of operational recovery is present.

FFIEC Supervisory Policy SP-5 in Chapter 25 requires each serviced institution to evaluate the adequacy of its servicer's contingency plans. Also, it must ensure its contingency plan is compatible with the servicer.

Retention schedules for automated records are generally determined on a case-by-case basis, since the amount and type of record duplication varies from site to site. The only way to provide sufficient protection of records is to continually review the flow of documents, data and reports, and to retain the necessary records for a certain time period until more current data is available to replace it. Some records may be available in both hard copy and machine-readable formats, with the latter being the preferred format.

Hard copy, while not preferred, is often the only record available due to cost or processing considerations. In addition to the types of records being backed up, the number of existing generations of particular information and the ability to recreate current versions from older versions should be considered. Certain records have use beyond the need for reconstruction of current records. After retention for backup needs, month-end, quarter-end, and year-end files can be further used to meet reporting requirements of the institution or regulatory authorities.

Another factor to consider regarding record retention is the location of the information processing center. If the center is located in a adjacent building, the possibility of a disaster occurring to both organizations simultaneously increases. This situation may necessitate that additional record protection procedures be instituted by the servicer or the financial institution. In this case, the importance of both parties' off-site backup materials is increased.

If a major disaster occurs, computer facilities may not be available, even if the servicer has duplicated the records on machine-readable media. Therefore, an alternate form of remote record storage that can be manually processed should be considered. Scanning or microfilming all items before being sent to the processor would protect the serviced institution should any items be lost, misplaced, or destroyed. Optical disk storage offers a viable alternative for mass data storage and retrieval after processing has occurred.

A number of records storage firms offer remote storage at a reasonable cost. Such firms can assist in developing a comprehensive microfilm or optical disk-based record protection program. User management, on the other hand, may wish to develop its own plan.

When internal processing is used, all of the information protection measures are developed and implemented by the institution. In servicing arrangements, the institution depends upon a second party to perform these activities. Whether the institution processes its own data or uses an outside servicer, it is crucial that the financial institution develop and implement a workable disaster plan.

See Chapter 13: Operations, Chapter 15: Network - Client/Server, and Chapter 16: End User Computing for additional information on alternate backup arrangements and record protection.

CONTRACTS

A poorly written or inadequately reviewed contract can be troublesome for both the serviced financial institution and the servicer. To avoid or minimize problems in such a contractual arrangement, legal counsel familiar with the terminology and specific requirements of a data processing contract should review it to protect the institution's interests. This may require hiring a knowledgeable outside attorney. Since the contract sets the terms of a multi-year

understanding between the parties, all items agreed upon during negotiations must be included in the final signed contract. Verbal agreements are not enforceable, and the inclusion of wording in the contract to the effect that no oral representations apply may protect both parties from future misunderstandings.

The contract should establish baseline performance standards for information processing services. In addition, the contract should define each party's responsibilities and liabilities, where possible.

Contracts between financial institutions and external information processing companies do not have a standard form, but rather they share a number of common elements. The contract should be viewed in its entirety, and evaluated in light of the substance and impact of its meaning, as well as the technical rights, obligations, and relief contained in it.

Minimum necessary contract elements and considerations are as follows:

1. A description of the work to be performed by the servicer.

    - Applications to be processed and services to be provided should be enumerated in, or as an appendix, to the contract.

    - The contract should contain provisions which define the responsibilities of both parties regarding the addition of future applications or the deletion of current applications. The parties' abilities and rights in modifying services performed under the contract should be fully detailed.

    - Processing frequency and report generation should be addressed. Master files updating and the holiday and weekend schedule should be specifically addressed.

2. The basis of costs, including development, conversion and processing, and additional charges for special requests.

    - Monthly processing fees should be fully enumerated. Additional charges and free services discussed in negotiations must be incorporated into the fee schedule. And, the basis of fee calculations should be disclosed.

    - If special software is developed for the institution to process its applications, ownership of these programs should be addressed. Generally, the developer of the software owns the product and can therefore sell or license it to other organizations.

    - The cost of converting the institution's records should be specified. In some circumstances, a portion of this cost is included in the monthly processing fees. If this is done, the servicer will want a contract term long enough to recapture conversion costs. In other situations, conversion costs are absorbed by the servicer. In most arrangements, negotiated costs of conversion are paid outright by the institution.
    - The time frame for conversion should be well defined so the institution can prepare its staff and facilities.

    - Costs for satisfying special management requests, audit needs, and regulatory requirements should be included in the contract.

3. Concerns regarding on-line communications availability, transmission line security, and alternate data entry.

    - Operating hours for the on-line communication network should be specified. Cut-off times for item capture and file maintenance entries should be included in the contract. If physical shipment of items to the servicer is performed, the cut-off time for inclusion in the current day's processing should be addressed, as well as the time frame for delivering reports to the serviced institution.

    - Responsibilities for security of the communications network should be addressed. Security software is now a common on-line control, and should be evaluated when choosing servicers. In many cases, message authentication can be used. This method provides certain benefits: Messages garbled during transmission may have sufficient data

for reconstruction; coverage is host-to-host so that all parts of the network are covered; and, while the messages are not private, message alteration can be determined. It also is possible to provide maximum security through a combination of these methods; however, this generally would be reserved for critical, large-dollar funds transfer areas.

4. Audit responsibility and the right of user representatives to perform audit procedures.

   - The contract should identify: Whether the servicer will contract for and provide copies (to the user) of a third-party CPA review, and at what cost (if any); the timing, frequency, and type of external audit coverage that the servicer will contract for; whether the servicer will maintain an internal audit function; whether the serviced institution, alone or with other serviced institutions, will contract for a third-party CPA audit; also, when and under what conditions the client is allowed to conduct audits of the service center; or, whether the institution will conduct servicer audits with its own staff.

5. Backup and record protection provisions (covering equipment, program and data files) to ensure timely processing by the service center in emergencies.

   - Contract terms should address the servicer's backup arrangements. Areas to be covered include all or a portion of the following. For on-line systems, it should be noted whether redundant files are maintained at the servicer or at a remote location and whether alternate telecommunication or processing facilities are available. For batch systems, it should be noted whether: alternate methods of transporting or rerouting document flows are available; off-site data files are maintained; or alternate computer processing sites are available. The servicer's software should be backed up, along with all necessary documentation. If the software is under a third-party escrow agreement, such arrangements should be detailed.

   - Backup arrangements should be addressed as part of the agreement. Contract terms may state only that adequate backup is maintained by the servicer, with specifics included in an appendix.

   - The servicer must have an effective disaster recovery/contingency plan. The serviced institution should receive a copy of the plan. A detailed description of the disaster recovery plan test results should be provided annually by the servicer to the financial institutions. Areas where protection of the serviced institution's records are not well defined should be clarified in the contract.

6. Establishment of liability for source documents while in transit to and from the service center. If the service center is responsible, the servicer should have adequate insurance coverage for such liabilities. Maintenance of adequate insurance for fidelity, fire, liability, and data losses from errors and omissions should be addressed.

   - Insurance protection maintained by the servicer should be reviewed to determine what additional coverage should be requested of the servicer or maintained by the serviced institution. Gaps in insurance protection generally account for little savings to the institution but could potentially be responsible for large losses. The institution should consider, and dismiss if appropriate, the option of self-insuring.

7. Confidential treatment of records. The servicer should be willing to protect the institution's data from unauthorized disclosure. Information which is sensitive or could be misused should receive a higher level of protection.

8. Upon the contract's termination, ownership of computer programs and related documentation, and of master and transaction data files in their machine-readable format, and the institution's right to receive these materials, should be addressed. The specific cost of returning institution data and the time frames for their return also should be clearly described, including any transitional assistance from the servicer and its cost.

9. Price changes and costs should be included. Provisions for contract cancellation or withdrawal from the servicing arrangement by either party,

including those covering adequate notification also should be addressed.

- The servicer may be allowed to raise fees to offset normal operating cost increases during the life of the contract. At the same time, the institution has the right to expect the costs of the contracted services to remain stable. Including parameters within which costs may increase provides both parties a measure of protection. Limiting the percent of allowable increases and giving the institution the ability to terminate a contract for excessive increases without penalty is desirable. The institution's obligation to pay outstanding invoices for services provided and the amount of penalty for early termination of the contract should be stated.

- Time frames for, and methods of notifying both parties of contract termination should be stated. If early termination is allowed, costs that the servicer had postponed for conversion or other activities should be recoverable.

- Time frames should be long enough for the serviced institution to allow orderly conversion from the present servicer to another vendor.

- Some service contracts contain silent renewal features which automatically renew the contract for either its original term or a given term without any explicit action of either party. Often, such silent renewal features are triggered six months to one year from the contractual expiration date of the original agreement. Financial institutions should be aware of such renewal features in service contracts.

10. Processing priorities should be detailed in the contract for both normal and emergency situations.

11. The contract should provide notification by the service center to the institution of all systems changes that would affect procedures, reports, etc.

12. The contract should provide that financial information be provided periodically (preferably annually) by the servicer to serviced institutions. In large corporate organizations, where the information processing servicer activities are a small portion of the total income and expenses of the corporation, the profitability and, therefore, the continued existence of an information processing subsidiary may not be well presented in an annual report. A breakdown of the subsidiary's balance sheet and income statement should be obtained. In addition, audited financial statements are of greater benefit to the financial institution than unaudited financials.

    - If the servicer charges the client for copies of periodic financial statements, this should be recited in the contract.

13. Training is an area where the institution can experience a large risk exposure. Improperly or inadequately trained employees can create situations which can be costly, in both time and money, to correct. Conversion of the institution's records should be preceded by careful planning and training. Smooth operation of the system and flexibility to handle normal operating problems require sufficient training. Abnormal or emergency situations require a higher level of training for perhaps a small group of employees. The amount, type, location and cost of training, and the number of employees to be trained should be detailed in the contract.

14. In addition to the concern of the serviced institution to protect itself through a well-reviewed and sufficiently amended contract, regulatory authorities have a contract concern regarding actions in the event of receivership. The contract should not contain special clauses which limit the ability of a regulator to arrange an orderly and reasonable conversion of data to another servicer or vendor, or to the receiver in the event of receivership. Merger, purchase, and assumption activities are hampered by excessive conversion penalties and fees. The requirement that the assuming or purchasing institution must pay the remaining balance of all monthly fees of a long-term contract reduces the ability of the receiver to provide swift and cost-effective reestablishment of

financial services to the community.

15. Contract and penalty provisions should be reviewed for reasonableness in: Length of contract versus postponed fees and charges; length of contract versus the reduction in the cost per month; establishment of large contingent liabilities through excessive penalty fees; compensation of the servicer for loss of income versus the penalty fees; and the punitive nature of penalty fees or clauses.

16. Contracts should provide a prohibition against the assignment of the contract by either party without the other's consent.

17. In some cases, servicers unbundle certain services and sell them as optional extras. This practice allows an institution to select only needed services. Tailoring services can reduce the overall cost of information processing activities. However, this practice is not acceptable when backup and data security are considered optional. These services should be mandatory because the institution which can least afford the cost of these services is also the one that can least afford not having them.

18. Finally, negotiations between two parties sometimes include the receipt of gifts, premiums, or bonuses for signing a contract for information processing services. These practices, although used in the commercial and industrial environment, are prohibited in the financial community by rules and regulations. The practice could be interpreted as bribery of a bank official rather than as a bargaining tool.

CONTRACT INDUCEMENT CONCERNS

Some financial institutions have signed servicing contracts that contain provisions that may adversely affect the institutions. Such contract provisions may include extended terms (up to 10 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 seem particularly attracted to these inducements.

Examples of inducements include:

- The servicer purchasing certain assets (e.g., computer equipment or foreclosed real estate) at book value, which exceeds market value.

- The servicer providing capital by purchasing capital stock from the institution.

- The servicer providing cash bonuses to the institution once the conversion is complete.

- The servicer providing up-front cash to the institution. The servicer states that the institution acquires the right to future cost savings or profit enhancements that will accrue to the institution as a result of greater operational efficiencies. These improvements are usually without measurable benchmarks.

- The institution defers expenses for conversion costs or processing fees under the terms of the contract.

These inducements may offer a short-term benefit to the institution. However, the servicer usually recoups its costs by charging a premium for the processing services it provides. These excessive fees adversely affect an institution's financial condition over the long-term. Furthermore, the institution's accounting for such inducements may be inconsistent with generally accepted accounting principles (GAAP) and regulatory reporting requirements.

Additionally, Title II of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) 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 (See Chapter 24 for

additional information and the legal cite).

Accordingly, when negotiating contracts, an institution should ensure that the servicer can provide a level of service that meets the needs of the institution over the life of the contract. It also is the institution's responsibility to ensure that contracts are accounted for in accordance with GAAP. Contracting for excessive servicing fees and/or failing to properly account for such transactions is considered an unsafe and unsound practice. In entering into service agreements, institutions must ensure that accounting under such agreements reflects the substance of the transaction and not merely the form. (See Chapter 25 for additional information on FFIEC SP-6: Interagency Statement on EDP Service Contracts.)

FINANCIAL INFORMATION FOR USER INSTITUTIONS AND SERVICERS

Many financial institutions have become so dependent on outside data processing servicers that any extended interruption or termination of service would severely disrupt normal operations. Termination of services generally occurs according to the terms of the service contract. Institutions also may experience termination of contracts caused by a physical disaster, such as fire or flood, or termination caused by bankruptcy. The serviced institution must prepare differently for each type.

The majority of terminations occur according to the terms of the contract. The contract should allow either party to terminate the agreement by notifying the other party 90 to 180 days before the termination date. This gives a serviced institution the time to shift to another servicer.

Termination caused by physical disaster occurs infrequently, but it may present the institution with a more serious problem than termination by contract. If the servicer has complied with basic industry standards and maintains a proper contingency plan, disruption of services to users will ordinarily be minimal. The contingency plan must require the servicer to maintain current data files and programs at an alternative site and arrange for backup processing time with another center. At a minimum, these provisions should allow the servicer to process the most important data applications. Since equipment vendors can often replace damaged machines within a few days, the servicer should be able to resume processing with little delay. The servicer, not the serviced institution, is responsible for the major provisions of the backup contingency plan. However, the institution must have a plan that complements the servicer's.

Termination due to the bankruptcy of the servicer is potentially the most devastating to a serviced institution. There may not be any lengthy advance notice of termination or an effective contingency plan because there may be no available servicer personnel. In this situation the serviced institution inherits the responsibility for finding an alternative processing site.

Although user institutions can ordinarily obtain data files from a bankrupt servicer with little trouble, the programs and documentation required to process those files are normally owned by the servicer and are not available to users. These programs are often the servicer's only significant assets. Therefore, a creditor of a bankrupt servicer, in an attempt to recover outstanding debts, will seek to attach those assets and further limit their availability to users. The bankruptcy court may provide remedies to the user, but only after an extended length of time to adjudicate substantive matters.

At this point, a serviced institution has two alternatives:

- Pay off the creditor and hire outside specialists to operate the center.
- Transfer data files to another servicer.

Either alternative is likely to be costly and may cause very harmful operating delays.

Therefore there is an emphasizes on the great importance to financial institutions of monitoring the financial condition of their servicer(s). In order to fulfill its fiduciary responsibility, a serviced financial institution will normally determine the financial viability of its servicer(s) on an annual basis. Once the review is complete, management must report the results to the board of directors or to a designated committee. At a minimum, management's review should contain a careful analysis of the servicer's

annual financial statement. Institution management also may use other forms of information to determine a servicer's condition. For example, reports of independent auditors and reports obtainable from appropriate regulatory agencies may contain information which can be vital in determining a servicer's financial condition. Managers also can use information provided by public media, such as trade magazines, newspapers, television, etc. If it becomes known that the servicer's financial condition is unstable or deteriorating, the serviced institution should put its contingency plan into effect. Even if the servicer remains in operation, its financial problems may cause it to take drastic measures that may jeopardize the quality of its service and possibly the integrity of the data in its possession. Institutions should consider a servicer's failure to provide proper financial data as an indication of unsound operating practices.

CONSIDERATIONS FOR SERVICE RECEIVERS

Senior management should review performance of the service provider. The review should cover:

- Financial condition.
- Costs.
- Ability to meet future needs.
- Quality of service.
- Control environment at the data center.
- Emergency backup provisions.
- Insurance requirements.

Problems in any area need to be discussed and a timely resolution sought. To help with the evaluation of the servicer, management should obtain all audit and examination reports available and review them thoroughly. Then, management should document their review and actions to substantiate this due diligence.

POTENTIAL SERVICE PROVIDER ISSUES

If a financial institution provides information processing services to others, it should examine the risks in doing so and the procedures in effect to minimize that risk. Although this subsection focuses on risks which may affect the institution providing services through a computer center, the effect on the customer institutions of obtaining information services in this matter should also be weighed. Primary considerations are:

- *Possible contingent liabilities* – The center must protect and properly process accepted work. The same controls used in processing the institution's work should be maintained when processing work for others.

  A well-written service contract with properly defined duties and responsibilities will protect both the servicer and the customer. Contract considerations are covered earlier in this chapter. In all cases, contracts should be reviewed by legal counsel familiar with computer service contracts.

  The service provider also incurs additional liability for ensuring adequate backup of programs and files is maintained.

  Contingency planning also must be expanded to coordinate with the serviced institution. Plans for obtaining input from and providing output to the serviced institution in a disaster/recovery situation need to be developed. The provisions of the plan which could affect client institution operations should be provided to the client institution. Also, the service provider should support the client's corporate contingency planning efforts in developing recovery procedures for a disaster at the client's facilities.

- *Insurance* – Financial institutions offering information processing services should be adequately protected by fidelity and other appropriate types of insurance coverage. (Insurance is discussed elsewhere in this section and in Chapter 9, Management).

- *Investment in equipment, software, and personnel* – In some instances, financial institutions make sizeable investments in equipment, software, and personnel to support customer servicing. This practice may represent a costly diversion from the primary business of a financial institution,

especially a small institution. Additionally, rapidly changing technology can render obsolete an institution's investment in information processing assets.

- *Costs* – Often new business is generated, or old business retained, due to the availability of IS servicing for customers. The cost of providing these services should not exceed the revenues generated; however, the institution must decide whether processing services are offered to generate income or to serve other less tangible purposes.

Frequently, income received from such services may more than offset additional operating expenses. Management should establish a formal method for determining costs and setting fees. Some institutions arbitrarily set their servicing fees at a level to meet or beat competition and to attract new customers, rather than establish fees based on a formal analysis of how their IS resources are used.

Economies-of-scale can be realized in equipment, facilities, and program development costs when processing assets are used by the financial institution to service others. Software development costs can be spread over a number of institutions, allowing maintenance of such programs to be a normal function of information processing, rather than specialized customer servicing.

Financial institutions sometimes offer a tailored or specially developed application to customers. However, the service must be priced to reasonably recover the development cost either initially or as part of the monthly servicing fee.

Excess equipment capacity can become a problem if it was acquired specifically for customer servicing. Normally, additional staffing will be needed, and unless these expenses can be offset by similar income increases from customers, a significant drain on the earnings of the servicing institution can result.
An IS operation consisting solely of one set of standardized applications is easier for management to control and administer.

- *Quality of service* – The quality of service offered to outside organizations is not always easy to assess. However, some complaints can be heard through discussions with the customer service representatives or the correspondent departments. In addition, the processing center should maintain a complaint file. Any complaints received should be thoroughly investigated and resolved by the servicing institution. The quality of servicing also can be monitored by reviewing customer contract cancellations, renewal rates, and payment delinquencies.

- *Control of documents* – If the service center prepares checks or other negotiable documents, the blank stock should be adequately controlled. Facsimile signature plates should not be maintained under the sole control of persons involved with center operations.

- *Billing* – When a financial institution provides services to other financial institutions, the receipt of service center income should be handled by a department other than the IS organization. This provides better separation of duties. The computer system should accumulate activity counts and would likely generate billing. Also, cost accounting data should be maintained so that center management can decide about future application services. In a holding company environment, the appropriateness of fees charged to subsidiaries should be reviewed.

- *Audit* – The internal auditor should compare, at least annually, customer service billing against IS activity records and comparative income and activity reports. A representative number of entries should be traced from source to payment. Also, it should be determined that customer records, supporting programs and documentation are afforded the same level of security and access control as the servicer's records.

POTENTIAL SERVICE RECEIVER ISSUES

If a financial institution receives information processing services from others, it should examine the risks in doing so and the procedures in effect to minimize that risk . Management's primary considerations should be to:

- Assess the types and levels of risks associated with information systems services received.

- Assess the adequacy of the system of controls safeguarding the integrity of the data processed by

the service provider.

- Develop, implement, and test contingency plans that will ensure the continued operation of the institution's data processing tasks/needs in the event of unforeseen events. Contingency plans should address both a disaster at the service receiver's facilities and a disaster at the service provider facility.

- Implement an effective system to monitor the financial condition of key data processing servicers.

- Expanded audit function to review controls at the service provider's facility if an adequate audit is not performed via a third-party review or some other acceptable means.

This section is intended to identify services provided to financial institutions and/or other businesses and to evaluate the adequacy of controls over these services. If information processing services are not provided to other corporate entities (including affiliate organizations), completion of this section is not required. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

Tier I

1. Obtain a list of services performed by the information processing center.

   a. For each serviced financial institution include:

      1) Type of charter.

      2) Name and address (city, state).

      3) List of applications performed.

   b. For nonfinancial customers include:

      1) Services provided.

      2) Number of customers for each service.

   c. Indicate if any customers included under (a) or (b) are affiliated with the service center.

2. Determine the level of servicing provided to others. Note if the service includes:

   a. Inputting customer information at the servicer's location.

   b. Inputting customer information at the customer's location (RJE - Remote Job Entry).

   c. A facilities management operation.

   d. The sale of hardware, software, or both.

   e. Support and maintenance of hardware or software products.

3. If servicer is a financial institution, determine if services performed are in compliance with all applicable regulations, such as the Bank Service Corporation Act, and Sections 23A and 23B of the Federal Reserve Act. (See Chapter 24, Laws and Regulations).

CONTRACTS

4. Determine if written contracts are in effect for all customers.

5. Review a copy of the contract(s) used and determine if they are in conformance with the guidelines contained in this *Handbook*.

SERVICE QUALITY

6. Determine if the level of service is acceptable by:

   a. Reviewing management reports. (Daily service logs, quality indicator reports, etc.)

   b. Reviewing the customer complaint file and the methods used to handle complaints.

   c. Reviewing customer payment records for any payments made under protest.

   d. Reviewing the minutes of the User Group if applicable.

7. Review management reports used to monitor the customer service function. Determine whether information received by customer service representatives is appropriately categorized, summarized, and used to provide feedback on problems encountered, user training weakness, customer service requests, etc.

CONCLUSIONS

8. Review the results of work performed in this section and in sections for Examination Planning, Internal/External audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers

should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

9. Discuss with management:

   a. Violations of law, rulings, regulations, or significant internal control deficiencies.

   b. Recommended corrective action for deficiencies cited.

   c. Management's proposed actions for correcting deficiencies.

10. Assign rating. (See Chapter 25 for additional information on FFIEC SP-2: Uniform Interagency Rating System for Data Processing Operations.)

11. Prepare an index of workpapers for this section of the workprogram.

12. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations. (See Chapter 2 for additional information on supervision by risk and supervisory strategies.)

13. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

CONTRACTS

1. Do contract provisions specify:

   a. Specific work to be performed by the servicer?

   b. The basis of costs, including development, conversion and processing, and additional charges for special requests?

   c. The established time schedules for receipt and delivery of work?

   d. Responsibilities for security of the communications network?

   e. Audit responsibility, including the right of user representatives to perform audit procedures?

   f. Backup and record protection provisions (equipment, programs, data files) to ensure timely processing by the service center in emergencies?

   g. Servicer disaster recovery plans are provided to the serviced institution for review?

   h. Provisions for sharing disaster recovery plan test results with serviced financial institutions.

   i. Liability for source documents while in transit to and from the service center? (If the service center is responsible, the servicer should have adequate insurance coverage for such liabilities.)

   j. Maintenance of adequate insurance in case of data losses through error and omissions?

   k. Confidential treatment of records?

   l. Ownership of computer programs and related documentation?

   m. Ownership of master and transaction data files and their return in machine readable format upon the termination of the contract or agreement?

n. Price changes, cost and method of canceling the contract, including adequate time allowance?

o. Processing priorities?

p. Notification from the service center to the users of all changes that would affect procedures, reports, etc.?

q. That financial information is to be periodically (preferably annually) provided by the servicer to serviced institutions?

r. Training provisions, including cost, for financial institution personnel?

s. Allowable actions in the event of receivership or bankruptcy?

t. Penalty clauses, if any, for early cancellation of the contract?

u. Prohibitions against assignment of the contract services by either party without the prior written consent of the other?

2. Do the terms of the contracts provide adequate protection and establish limits of liability for both the servicer and the user?

SERVICE QUALITY

3. Are services performed according to the contract terms?

4. Does the service center maintain a customer complaint file?

5. Does the center investigate and attempt to resolve all complaints received?

6. Do exception reports meet the needs of the users?

7. Are users provided training to understand each automated application commensurate with their job responsibilities?

	Comments
8. Are customers provided with current user manuals? Does each user manual cover: a. The preparation and control of source documents? b. Control, format and use of output? c. Settlement and reconcilement procedures? d. Data security responsibilities of serviced financial institutions?	
9. Proceed to procedure 8, Tier I.	

Examiner | Date

_____|_____

Reviewer's Initials

IS SERVICING – RECEIVER WORKPROGRAM

CHAPTER 22WP

(FILE NAME ON DISK # 3 = IS-WP#18.WPD)

COMMENTS

This section is intended to identify services received from financial institutions and/or other businesses and evaluate the adequacy of controls over these services. If information processing services are not received from other corporate entities (including affiliate organizations), completion of this section is not required. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

Tier I

EXAMINATION PLANNING

1. Review the following documents:

   a. The examination scope memorandum issued by the examiner-in-charge (EIC).

   b. Previous examination reports and working papers.

   c. Internal/external audits.

   d. Internal reports and any computer services policies and practices, including corporate contingency plans, information security practices, and end-user/microcomputer policies.

2. Determine any material changes affecting the institution's information processing function since the previous examination by reviewing pertinent internal files and correspondence.

3. Based on the performance of the previous steps and discussions with the EIC, determine the scope and set the objectives for this workprogram section. Select the worksteps necessary to meet examination objectives. Appropriate worksteps can include the following procedures, along with procedures discussed in the workprograms addressing:

   a. Corporate Contingency Planning.

   b. MIS Review.

c. Networking.

d. End-User Computing

e. Retail EFT.

f. ACH

GENERAL

4. If the institution receives major data processing support from one or more outside servicers.

   a. List the name(s) and location(s), of the servicer(s).

   b List any known affiliations between these servicers and either banks or data processing vendors.

   c. Prepare a listing of the services outside vendors provide the institution.

5. Determine if the institution is subject to notification requirements outlined in the Bank Service Corporation Act (See Chapter 24, Laws and Regulations for additional information on this act).

CONTRACTS

6. Review a copy of the contract(s) used and determine if they are in conformance with the guidelines contained in the narrative section of Chapter 22: IS Servicing - Providers and Receivers.

SERVICE QUALITY

7. Determine whether management obtains and reviews information detailing service quality factors. Sources of information could include:

   a. Reports detailing measurable performance indicators. (Eg., up-time, processing results vs. contract performance goals, etc.)

   b. Internal reports evaluating the provider's customer service department.

   c. Institution personnel participation in servicer sponsored or independent user groups addressing common client issues.

d. Employee feedback regarding training provided by the servicer.

FINANCIAL

8. Assess the adequacy of the institution's system for monitoring the financial condition of its servicer(s) and whether the system is sufficient to project the continued viability of contracted services.

   Review and assess the adequacy of any alternate processing plans management has for replacing servicers who reveal signs of financial weakness.

9. Does the institution pay IS related fees to affiliates, shareholders, or insider related companies?

   If so, does management review or audit these transactions?

   Are these transactions in compliance with applicable laws and regulations?

POLICIES AND PROCEDURES

10. Has the board of directors developed and implemented corporate policies or procedures which govern institutional information processing activities, including?

    a. Corporate contingency planning.

    b. End-user computing activities.

    c. Information security.

11. Has management evaluated the adequacy of contingency plans of its servicer(s)?

12. Has management ensured that the institution's contingency plan is compatible with and complements the servicer's?

13. Does management test the adequacy of its corporate contingency plans on an annual basis or in accordance with its plan?

14. Has the directorate reviewed and approved the corporate contingency plan within the last 12 months?

15. Do board minutes adequately reflect directorate approval?

16. Determine how management or the board of directors complies with regulatory policies involving EFT switches and network services. This may include review of outside servicers, including nonfinancial companies, who provide EFT services. It also could include controls over ACH, POS, ATM, or automated bill payment systems.

CONCLUSIONS

17. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

18. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

19. Assign rating. (See Chapter 25 for additional information on FFIEC SP-2: Uniform Interagency Rating System for Data Processing Operations.)

20. Prepare an index of workpapers for this section of the workprogram.

21. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations. (See Chapter 2 for additional information on supervision by risk and supervisory strategies.)

22. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

CONTRACTS

1. Do contract provisions specify:

   a. Specific work to be performed by the servicer?

   b. The basis of costs, including development, conversion and processing, and additional charges for special requests?

   c. The established time schedules for receipt and delivery of work?

   d. Responsibilities for security of the communications network?

   e. Audit responsibility, including the right of user representatives to perform audit procedures?

   f. Backup and record protection provisions (equipment, programs, data files) to ensure timely processing by the service center in emergencies?

   g. Servicer disaster recovery plans are provided to the serviced institution for review?

   h. Provisions for sharing disaster recovery plan test results with serviced financial institutions?

   I. Liability for source documents while in transit to and from the service center? (If the service center is responsible, the servicer should have adequate insurance coverage for such liabilities.)

   j. Maintenance of adequate insurance in case of data losses through error and omissions?

   k. Confidential treatment of records?

   l. Ownership of computer programs and related documentation?

   m. Ownership of master and transaction data files and their return in machine readable format upon the termination of the contract or agreement?

n. Price changes, cost and method of canceling the contract, including adequate time allowance?

o. Processing priorities?

p. Notification from the service center to the users of all changes that would affect procedures, reports, etc.?

q. That financial information is to be periodically (preferably annually) provided by the servicer to serviced institutions?

r. Training provisions, including cost, for financial institution personnel?

s. Allowable actions in the event of receivership or bankruptcy?

t. Penalty clauses, if any, for early cancellation of the contract?

u. Prohibitions against assignment of the contract servicing by either party without the prior written consent of the other?

2. Are the terms of the contract appropriate?

3. Did the initiation/continuation of the contract provide any inducements?

   a. If yes, were the inducements properly documented?

   b. Were the inducements appropriate?

FINANCIAL

4. Does the institution's policies, practices, or procedures for monitoring the annual financial performance of its major data processing servicer(s) include:

   a. Reviewing financial information.?

b. Reviewing reports of independent auditors?

c. Reviewing regulatory reports?

d. Reviewing public media (trade papers, TV, etc.)?

e. Presenting the results of these reviews to the board of directors?

AUDIT

5. Does the internal/external audit coverage of the data processing function reflect:

   a. The absence of conflicting duties (independence)?

   b. Sufficient training and experience of auditors (competency)?

   c. An adequate scope?

OPERATIONS

6. Do policies or practices adequately segregate personnel duties and responsibilities in the areas of:

   a. Input preparation and balancing?

   b. Data entry?

   c. Reject reentry?

   d. Balancing of output?

   e. Handling of unposed items?

7. Do procedures or practices for master file change requests (address changes, due dates, interest rates, etc.) address the following:

   a. Require documentation sufficient to document the substance of the transaction?

   b. Identify the originating personnel?

   c. Reconciling of the change report by an independent individual?

8. Are management or the board of directors regularly reviewing exception reports?

9. Does the institution microfilm or otherwise record source documents before the documents are transported to the data center?

10. Are computer-processed negotiable instruments (e.g., blank checks, stock certificates, plastic bank cards) and facsimile signature plates:

    a. Under dual control?

    b. Kept in a locked, secure location?

    c. Issued only as required?

    d. Prenumbered and in sequential order?

    e. Governed by logs that provide for an acceptable audit trail?

    f. Reconciled after each use?

    g. Periodically inventoried?

11. Are listings of unposed entries used to control resubmissions?

12. Are rejected items and lists of captured items independently balanced?

13. Is the operation of equipment limited to personnel who do not perform conflicting duties?

14. Has the institution adequately trained a sufficient number of employees to operate the equipment and thus reduced its dependence on key personnel?

15. Are output reports balanced to general ledger control on a daily basis?

INFORMATION SYSTEMS SECURITY

16. Identify persons with the authority to administer the organization's information systems, and:

a Determine if the number of personnel with security administration authority appears reasonable, given the size and complexity of the institution. Management should limit the number of those persons with security administration authority to only those who are necessary to provide primary and secondary security coverage.

b. Ensure that management limits security administration responsibilities to only those individuals who do not have other conflicting duties.

17. Has senior management provided its primary security administrator with an approved listing of those individuals authorized to grant personnel access to the system?

18. Do security administrators maintain written access authorizations for all users?

    a. Obtain a listing of existing users from the security administrator.

    b. Compare written access authorizations to the listing of resident users.

19. Obtain a listing of all available security exception reports. Determine which exception reports management is utilizing and the individuals responsible for their review.

20. Ensure that the institution's exception report review process appropriately supports relevant separation of duty issues.

INSURANCE

23. Obtain a listing of all information system-related insurance coverages. Determine if contracted coverages are sufficient to comply with the guidelines set forth in Chapter 9, Management.

24. Proceed to procedure 17, Tier I.

Examiner | Date

_____|_____

Reviewer's Initials

COMMUNITY FINANCIAL INSTITUTION IS EXAMINATION PROGRAM CHAPTER 23

(FILE NAME ON DISK # 2 = S2C23.WPD)

COMMUNITY WORKPROGRAM

The Community Financial Institution IS Examination Workprogram in smaller serviced institutions helps determine if controls are adequate for evaluating and controlling IS risk when selecting a servicer, signing data processing contracts, establishing IS controls in user departments, establishing microcomputer controls, and developing and testing a disaster contingency plan. Use of either procedure ensures that IS risk is periodically evaluated in all institutions. The findings and conclusions of this program are included in the safety and soundness ROE, as appropriate.

The Community Financial Institution IS Examination Workprogram helps the examiner evaluate IS related internal control procedures in smaller financial institutions using vendor supplied and supported software. In all cases the use of the FFIEC Community Financial Institution workprogram is predicated on the fact that there is no on-site systems and programming activity being performed either by IS staff or by private consultants. If the original vendor who supplied the software has access to the institution's operating or program software through an offsite networking hookup offsite, more extensive review procedures must be employed. This workprogram also should not be used whenever the institution under examination provides any significant IS services to another nonaffiliated institution(s). The FFIEC IS Examination Workprogram should be used for IS examinations when more detailed examination steps are appropriate.

The community financial institution workprogram contains general instructions and a series of work steps to be performed before answering questions. There is a cross-reference table at the end of the work program that relates the location of the primary initial reference for that work steps. The reference is pointed to the appropriate section, by the chapter and page number located at the bottom center of the page.

INTRODUCTION

Technological advances in recent years have given rise to smaller yet more powerful computer systems. Effective interaction with most systems now requires only a modicum of computer knowledge and takes place through menu programs or graphical user interfaces. Pricing for many computer systems has decreased to a point that is within the capabilities of most, if not all, financial institutions. Many small financial institutions (community bank/thrift) have taken advantage of technological advances and purchased in-house, or turnkey, computer systems.

Essentially, a turnkey system consists of a purchased software application that, when installed on appropriate hardware, typically requires only modification of parameter tables and loading of an institution's financial data before processing can begin. The parameter tables may be interest rate tables, service charge tables, interest charge methods, etc., that programs will retrieve values from to apply in various data manipulations. Generally, no additional program modification must be accomplished. Turnkey systems vary in complexity and some may require extensive data processing knowledge to operate and maintain. Progressive institutions with aggressive business plans may require several experienced data processing personnel to manage the systems as they become more complex. Ultimately, the decision to acquire a turnkey system should be made after careful analysis and evaluation of pertinent facts.

Many of the issues related to larger, more complex information systems discussed in other sections of the Information Systems Handbook are basic tenets and also apply to smaller systems. The remainder of this chapter will discuss issues germane to smaller, turnkey systems.

RATIONALE FOR ACQUISITION

Many factors may give rise to the desire to obtain a turnkey system. Generally, the need or desire to acquire a turnkey system will result from one or more of the following reasons:

- Financial institution operations and advancement into new commercial areas may be inhibited by the servicer's inability to adapt.

- The current servicer is not responsive to institutional request for enhancements.
- The cost of services rendered the financial institution have become excessive.
- The servicer may be ending services partially or completely.

In the latter case, financial institution managers may be faced with the need to acquire processing capability rapidly, especially if the servicer is curtailing operations due to financial failure.

EVALUATION OF SYSTEM REQUIREMENTS

To facilitate the evaluation and decision process, a committee consisting of users and managers should identify system requirements. It is important that an institution's end-users be involved in the process. They can provide valuable information regarding current problems and what would enhance processing. Not including them may result in their failure to provide important information and could result in resistance to change. Additionally, there must be a thorough understanding of the initial and continuing costs associated with the acquisition of an in-house system. Normally, the committee's findings are reported to the board of directors for ultimate review and acquisition approval.

FEASIBILITY STUDIES

Very few financial institutions rely on manual systems for information processing. Most either receive data processing services from a third-party provider to meet their particular needs, or they have acquired an in-house system. As previously mentioned, the decision to acquire a turnkey system should be supported by a thorough analysis and evaluation of relevant facts. This is probably the most critical step in the entire process. It is in this step that the evaluation and recommendation for system approval will be completed. Faulty analysis may result in an undesirable system that fails to meet management's expectations. The inaccurate determination of costs involved may adversely affect an institution's earnings and ultimately capital. For those reasons, among others, the cost of a thorough feasibility study will be minor in comparison to the funds spent on a system that does not fulfill expectations.

Feasibility studies are the prime method for evaluating the suitability of solutions to particular problems. Refer to initiation of a feasibility study, management should have a clear understanding of what the current problems are and what constitutes the desired remedies. Without this information, effective solution is unlikely.

The degree to which any feasibility study needs to be conducted will depend on an institution's specific needs. The study may be completed by in-house personnel, but it is not unusual for specialized consulting firms to assist. System vendors for turnkey solutions also may provide consulting services. However, management must remember that some consultants have an interest in increasing the installed base, and may not be unbiased in the recommendation of a system.

HARDWARE AND SOFTWARE CONCERNS

Software Evaluation

System acquisition should focus on the most important part of the system – the software. Too often the emphasis is on finding a computer and the importance of the software is overlooked. Software consists of a set of instructions that can be executed by a computer. The software should be thoroughly evaluated to determine that it will meet the institution's current and future needs. Once an institution has tentatively identified a suitable software package, a good step to take would be to contact current users of the product and ascertain their satisfaction. User groups also may provide good information on the functionality of the product and responsiveness of the vendor to users' needs. Examiners should review management's software evaluation process to gain a further understanding of selected packages' suitability.

Audit Trail Considerations

Software for financial institutions should provide the capability of auditing transactions if financial information in monetary accounts will be manipulated. Clear audit trails should be produced as transactions take place. The ability to obtain reports detailing transaction activity should be part of the standard software. The reports should contain the date, time, type of transaction, terminal from which the transaction was initiated, and the identification of the person initiating the transaction. The software's intrinsic ability to produce adequate reports, or the existence of an add-on package through which suitable reports can be generated, should be evaluated by examiners. The lack of adequate report generation

capabilities will limit the value of the information system to management and should receive adverse commentary in the IS Report of Examination.

Software Costs and Use Rights

The cost of software will vary with the complexity or size of the institution. Normally, software is not purchased and the financial institution obtains no ownership rights. Rather, the software developer licenses the user and allows the user certain rights to the software. Depending on the particular software, license rights may reach multiple thousands of dollars and will be granted for a specific period of time. There may also be an annual fee associated with the software use. Periodically, new versions, or releases, to the software will be provided.

Program Modifications

Since most turnkey software packages are developed for the express purpose of installing it in multiple institutions, most vendors offer custom program changes to adapt the package to meet certain user needs. Some minor alterations may be provided at no charge, but users should expect to incur additional expense for most software changes. Periodic vendor initiated enhancement to the software should be expected. These changes may result from the institution of new laws and regulations that require them. Or, the changes may be at the request of user groups that are experiencing problems or want software enhancements. Such changes may be included without additional cost in the periodic routine software upgrades as long as they are improving the generic software package and are not particular to any single institution.

Hardware Selection

After a suitable software package has been selected, a determination on the necessary hardware can take place. This normally will not pose a significant problem from the selection standpoint. Since the software vendor will know what hardware best runs the software, some selection decisions may already be made. Many of the software vendors either sell the entire package which includes hardware, or work closely with other vendors that do. Costs and services vary and management should evaluate suppliers to obtain the most favorable terms.

Purchasing and Leasing Hardware

Hardware, like software, may be leased or purchased. The initial cost of purchased hardware may be significant and will depend on the system design. Amortization of the cost for such equipment usually should take place over a period of time not longer than seven years. A review of the actual method employed by a financial institution should take place during an examination.

Leasing takes on more favorable attributes in the opinion of some managers. The system cost can be apportioned over the lease period and remains somewhat constant. Then, at the end of the lease period, management normally has the option to continue utilizing the equipment on an extended lease, purchase the equipment at a specific value, or arrange for new equipment. Managers and examiners should thoroughly review the acquisition of equipment. This is especially necessary when the institution is upgrading hardware systems, and the old hardware will be purchased by the current or new vendor as part of the sales agreement. Such transactions have given rise to excessive costs for new equipment based on inflated purchase costs. If abuses are found, such transactions should receive unfavorable commentary in Reports of Examination. Additional guidance may be found in the FFIEC Supervision Policy 6 (SP-6), Interagency Statement on EDP Service Contracts. Although SP-6 primarily focuses on service providers, the same general problems may exist in lease agreements or repurchases of used computer equipment.

Maintenance Concerns

Computer systems are predominately electronically oriented, but many of the system components have mechanical or moving parts. This gives rise to the need for a sustained maintenance program to minimize the probability of an equipment failure. Normally, operators can perform the majority of routine maintenance on equipment such as tape drives, reader/sorter devices, and other mechanically oriented equipment, but some required maintenance is best performed by individuals that specialize in such matters. Management should be aware that a continuing commitment is made when hardware is acquired through lease or purchase. Replacement and maintenance cost considerations should be a part of

any decision to purchase or lease equipment.

Vendor Stability Evaluation

The acquisition of a turnkey computer system generally entails significant costs and requires certain levels of knowledge regarding the system. Financial institution management may place a considerable reliance on the various vendors for technical support and overall assistance. Some of the knowledge necessary to evaluate a particular vendor's stability may be gleaned from overall dealings with the vendor during the product evaluation phase of system selection. However, if reliance will be placed on the vendor for continued support, an evaluation of the vendor's ability to provide the necessary support should be made. This can best be accomplished by reviewing the financial strength of the vendor. This may be complicated by the very nature of the vendor.

If the vendor is part of a larger organization, financial statements may not segregate that particular segment of operations making the evaluation difficult. Companies that are not publicly traded may not willingly provide access to financial information. This does not imply that these companies are not strong and capable of withstanding business cycles. But, the inability of management to adequately evaluate these companies should indicate caution is necessary when determining their continued support, potential. The evaluation should not end once the acquisition has taken place. Periodic evaluation should take place for any support vendor management relies on. Appropriate documentation to substantiate the review should be maintained. Management's analysis should be reviewed during examinations.

Facilities

In addition to ensuring that appropriate equipment and software are obtained, management must be concerned with providing an adequate environment in which to process work. Depending on the nature and extent of the system chosen, alterations may entail only a slight rearrangement of work areas. If a physically larger system is acquired, the construction of a segregated area with a special environmental control system may be necessary. Some controls and features are discussed in the following paragraphs.

Equipment Floor Plans

The location and arrangement of the system should take into consideration the work patterns of people and the flow of documents. It is not advisable to have large numbers of people consistently traversing the area where computer operations take place. Such presence provides a heightened potential for accidental damage to systems and the potential to lose information. Preferably, the computer system should be in an area that is away from the general public and access to the area restricted to only necessary personnel. Workflow, or document flow, also should be considered to enhance efficiency. Arranging the processing operation and equipment to facilitate workflow should result in a smoother and less time consumptive environment.

Noise Considerations

The physical environment may require special considerations. With the exception of any reader and sorter equipment, these smaller microcomputer based systems are not generally noisy. High speed impact printers are exceptionally noisy. If they are utilized, sound dampening covers may be necessary. As a result of the size and type of various peripheral devices in use, significant noise may be created during normal operations. Without a special facility to house the equipment, the noise may be disruptive to other workers in the area.

Environmental Controls

Small systems, some of which may be run on very powerful microcomputers, will generally only need an environment that is suitable to humans. These systems are very tolerant of a wide range of temperatures and conditions. Larger systems may require special environments where climate and humidity control are necessary. Computer systems also are capable of generating significant amounts of heat. Failure to adequately maintain suitable temperatures within the operating environment may result in system failure and loss of data.

Fire Detection/Suppression Considerations

No matter what the system size, adequate protective systems must be maintained. Fire protection systems for smaller, microcomputer based systems, may consist of hand-operated fire extinguishers. These extinguishers should not be dry chemical. The release of the contents of the extinguisher could cause more damage than the small fires they are designed to extinguish. Larger, specialized facilities most likely will require a more sophisticated system such as halon or its replacement gas, FM200. These central

suppression systems are costly to install and maintain. They may often be supplemented by hand-held extinguishers.

Library Facilities

Adequate facilities for tape and disk storage should be provided. The storage facility also should be protected by a fire protection system and have limited access. Because this area will house numerous different tapes, disks, or cartridges, each item should be clearly marked to ensure that the contents are known.

Physical security

No matter what the system size, adequate security for the facility must be in place. Fire detection systems should provide local notification and it is preferred that they also notify either a monitoring entity or fire department. Intrusion alarms should be connected to a 24 hour monitoring facility. Some smaller institutions have installed infrared sensing devices that monitor and provide alarm when temperature changes are detected. These are primarily intrusion detection devices, but because a fire would result in heat increases, the sensors will detect them also. While a fire would trigger an alarm, it would signal an intrusion alarm and a fire would most likely increase in intensity before the fire department could be notified and respond. Management should evaluate the need for protective systems. Generally, a schematic diagram of security and fire suppressions system will be available and sufficient in detail to allow an evaluation of these systems.

DATA CONVERSION

For institutions that have records on a manual system, loading information into the computer system for the first time will entail a significant amount of effort. The conversion may require and will probably be best completed by a phased conversion where specific files are computerized based on a targeted completion date. Due to the potential for significant losses during a conversion, extreme care must be taken to ensure that a thorough reconciliation of balances from manual records to computer records takes place. Where an in-house computerized system currently exists and a different system is being installed, conversion will consist of transferring data from one system to another. Most vendors will assist in the conversion and provide necessary programs to complete the conversion. As with the initial loading from a manual system, adequate reconciliation from the old system to the new system must take place. Because of the speed at which computer to computer communications can take place, the conversion may require considerably less time to fully implement. A thorough review of the conversion should be conducted during an examination. Particular attention should be given to the reconciliation process between systems. Management should consider parallel processing, if the capability exists. This would further ensure that the new system was functioning properly before shutting down the old system.

CONTRACTING FOR SERVICES

Because of the nature of many institutions, numerous services are contracted out. Any service provided to an institution for the acquisition, installation, or conversion of information should be pursuant to a written contract. The contract should cover all pertinent points and fully set forth requirements and expectations. Specific language should be included to facilitate an evaluation of the product or service relative to the terms of the contract for acceptance purposes. (Refer to Chapter 22, IS Servicing Providers/Receivers, for additional information on contracts).

DISASTER/CONTINGENCY PLANNING

Information and Data File Backup

No matter what the size and complexity of the system, adequate backup of system information must take place. Instructions for backup operations should be present and adherence to the requirements evaluated. Written procedures should outline the various frequency for backups and specify retention period for records. All media contents should be clearly marked. Retention periods should be sufficient to ensure that nomore need for the data can be anticipated before its destroyed. Management should ensure the backup media is stored in an alternate location. Under no circumstances should the repository for the backup media be the same location as the system from which it was taken. This would result in an unacceptable exposure to loss of all data and could render backup media useless.

Emergency and disaster recovery planning must be accomplished by all institutions and should consist of institution-wide recovery planning. FFIEC SP 5, “Interagency Policy on Contingency Planning For

Financial Institutions" provides general guidance to financial institution managers regarding contingency planning.

Emergency Plans

Emergency events may result in the temporary inability to utilize financial institution facilities, including the computer operations area. Example, would be a bomb threat or loss of power to the facility. Both of these events will disrupt data processing activities, but not preclude the resumption of the activities within the same facilities in a reasonable, and normally short, period of time. The disaster recovery plan would be directed toward situations in which the facilities may no longer exist or the perceived inability to utilize regular facilities for a protracted period of time exists. A major fire, earthquake, or flooding could render facilities unusable for significant periods of time. Under these conditions, management would need to re-establish operations at another location.

Emergency planning should consist of actions to be taken to prevent the loss of life, injury of personnel, prevent loss of data within the system, and when possible, conduct an orderly shutdown of the computer system. The plan should be written and all personnel should be familiar with it. There should be an annual test of the emergency plan to ensure all personnel know their responsibilities. The emergency plan may be a part of the disaster recovery plan.

Corporate Contingency Recovery Plan

The disaster recovery plan should be a financial institution-wide plan including recovery of information systems at a secondary site. The need for an elaborate plan will be dictated by the level and complexity of the information systems in use. The plan should be written and clearly state who has the authority to order the re-establishment of operations at the backup site. Since the declaration of a disaster may entail a significant fee where a structured recovery site is involved, this power should not be arbitrarily granted. Often, the plan will limit this to one person. While, in theory, this may seem suitable, criteria should be established that will let other people act. Otherwise, the implementation of plan may be delayed while attempts to contact the designated person take place.

Regular Testing Program

Familiarity with the disaster recovery plan is essential. When an emergency takes place, resumption of operations in a familiar environment is anticipated. The move to a backup site that would be required in a disaster is a re-establishment of operations in an entirely different location. Participants in recovery operations must know exactly what part they play and what actions they must carry out. It is important that the plan's annual testing incorporate all recovery team members to the extent possible.

Board of Director Involvement

Senior management and the board of directors should review and approve the plan. A subsequent review and approval of the plan should be conducted annually. This can be accomplished by ensuring that after the plan's annual test any necessary updating takes place. The test results and updated contingency plan can then be submitted for approval. All reviews and approvals should be noted in the institution's official records.

Examiner Review

Examiners must thoroughly review both the plan and any tests conducted to determine if they are realistic and implementable. Failure to have an acceptable plan or conduct an annual test will normally require adverse comments in the Report of Examination.

CONTINUING ISSUES AND CONCERNS

Audit Program

The need for audit exists in any system, manual or computerized. However, special skills may be required to effectively audit computerized systems. Some institutions may lack sufficient audit expertise to conduct effective information systems audits. When such is the case, external assistance from qualified audit providers should be obtained. Most institutions will possess the capability to implement some form of an internal audit program covering information processing systems. At a minimum, institutions should have processes to verify that interest calculations remain correct after parameter changes and that access to the information system is limited to those who require computer use. Examiners should thoroughly understand the level of audit performed for the information systems in use.

Audit Software

Audit software may be included as part of the particular software system a financial institution

purchases. There also are also audit software products produced by third party vendors for many systems. Audit software provides the capability to produce reports or records that can be used to verify information within the computers databases. Additionally, there are numerous report writer and query programs that can be used to produce audit reports. The query facility within the OS400 operating system is a prime example. Most examiners are familiar with the direct verification process for deposit or loan accounts. The verification notices are one product produced by audit software. When in use, all query report formats and programs utilized for auditing purposes should be strictly controlled. Ensuring the integrity of these programs is of paramount concern.

Systems and Program Maintenance

The nature of most turnkey or small computer systems implies that there is no programming activity at the institution. This is most often the case. Some people may consider the setting of program parameters, such as interest rates, to be programming. However, unless the alterations to the system result in actual changes to the logic, or way the system manipulates data, it is not considered programming. Program maintenance in the turnkey environment normally consists of updating particular vendor programs with a disk or tape sent to the institution for installation. In some institutions, management may allow the vendor to upgrade the programs via a remote communications package. In these instances, all remote access via dial-up modem should be pre-approved by management, and the upgrade activity needs to be thoroughly documented in a log book. In any case, parameter changes and program upgrades must be controlled. Only under extraordinary circumstances should the vendor be allowed unaccompanied access to the computer system. Once a computerized system is established, any changes to the system should only take place after management's approval has been obtained. Specific procedures, preferably written, should be in place, and adhered to, for any parameter change or system upgrade. These procedures should include a post-implementation review of the parameter changes made to ensure they were correctly applied. For example: changes in the calculation of interest, terms of instruments, etc. must be proper. This review should occur no later than the day following the change and be performed by an employee with a clear understanding of what was modified and that the expected results were achieved. This form of verification also may be coordinated with the audit department. Records of changes made should be maintained and available for examiner review.

Software Escrow Agreements

For institutions that do not purchase a source code, vendors usually have arranged for it to be held by a third party. The code would be available to the users under conditions specified in the license or escrow agreement. Examiners should be aware that when this situation exists, an audit of the software in escrow should take place annually. The audit should verify that the software held by the escrow agent is the latest version and that the source code is compilable and executable. Since vendors also offer some custom modification to the software packages, examiners should ascertain that copies of the custom code or altered programs also are safeguarded. Otherwise, the financial institution may be unable to restore the exact code to perform operations from the escrowed software.

While many vendors do not provide the source code to the institution, some vendors do place the source code on the system to facilitate corrections, enhancements, and resolution of problems. Examiners that encounter the source code on the institution's system, where programming does not take place, should determine why the code is there and how it is secured or access to it is restricted.

New Release Installation

As discussed earlier, most vendors periodically will update software to take advantage of new processes, correct deficiencies and problems, and generally improve the application’s utility. Sometimes, financial institutions do not upgrade to the new version. When this condition is observed within a financial institution, examiners should determine the reason management has chosen not to install the latest version. Failure to install periodic releases may result in difficulty when the institution has to install more recent versions with required changes in regulatory or other requirements. It is possible that before installing the most recent version, that all previous releases must be installed. This can be very time consuming and a sudden, significant expense for some institutions.

Many software vendors require installation of the periodic update that is normally near the end of the calendar year. This is due to changes normally made to facilitate end-of-year processing. Often, the new

version must be installed within a specific time period. This is frequently tied to the cut-off date after which the previous version may no longer be supported.

Appropriate Report of Examination commentary should be made where the failure to upgrade to most recent versions of software is discovered.

Continuing Evaluation and Planning

Management should periodically evaluate the capabilities of the information system relative to the institution's current business plans. Capacity planning should ensure that the growth in financial information does not exceed the system's capacity to maintain the information. Some software vendors stratify their software and license it to be used in financial institutions with specific levels of assets and or accounts. It is too late to begin planning when the recommended levels are exceeded. Management would be forced to react to a potentially critical event.

Because no system is designed to be the last one, management must have a system replacement plan. All systems will have an effective usefulness, if not functionally, then economically. Management must remain vigilant to the need to upgrade or replace outmoded technology and software. Failure to remain aware and take the necessary steps could result in an insecure or less than cost effective system.

Training

As with the need to maintain software and equipment, personnel also must receive periodic training to remain effective. Many features in computer systems are underutilized or not used at all due to the lack of understanding. Even smaller systems often provide features that could provide more utility if they were better understood. Management should provide periodic systems' training and ensure whenever new equipment or software is obtained, adequate training is provided to a sufficient number of employees.

Regulatory Examinations

The installation of computerized information systems may result in the institution being subjected to regulatory examinations. During these examinations, an assessment of the audit coverage, management, systems and programming, and computer operations activities will take place. An overall rating will normally be assigned to the Information Systems activities. These examinations usually will be conducted in accordance with the FFIEC guidelines with results reported to management at the conclusion of the examination. Examiners should communicate their findings with management during the examination process to facilitate better communication and corrective actions.

EXAMINATION PROCESS

FFIEC Community Financial Institution IS Workprogram and IS Report of Examination

The FFIEC has adopted a format for examining turnkey systems, the IS Workprogram for Community Financial Institutions. Each agency is responsible for guiding its examiners through the workprogram. All necessary areas are addressed by the workprogram, but it should be considered an evaluation tool only, not the end of the process. Negative answers on the workprogram may not indicate an undesirable condition in every institution. Compensating controls may be in place and alleviate the need for controls specified in the workprogram.

The FFIEC also has adopted a specific report format for Information System Examinations. The report has an open and confidential section. Generally, completion of the report is guided by FFIEC standard with minor deviation allowed by the various agencies.

Shared Application Software Reviews

Shared Application Software Reviews (SASRs) for the most widely used turnkey software packages are produced by FFIEC member agencies and are available for examiner use. These reviews provide a good overview of package features, and any systemic problems with the software. For areas identified as potential problems, examiners should look for compensating controls. They also may indicate problems that arise when particular hardware is used to run the package. Because the revision of most turnkey software is enhanced and known problems periodically corrected, examiners should not rely solely on problems noted in SASRs for report comments. A determination as to the existence of the problem in a specific institution must be made. Additionally, the SASRs are not, under any circumstances, to be released to the institution. They are for internal FFIEC member agency use only.

Segregation of Duties

Small financial institutions, the predominate users of turnkey systems, may lack adequate staffing to fully segregate duties and responsibilities. In such cases, additional precautions and controls should be established to ensure system integrity. These measures can consist of rotation of duties and additional audit coverage. Examiners should ensure these measures have been established and adhered to, but remember to be reasonable when requesting additional controls. At a minimum, management should ensure that an adequate number of employees receive training on the system to minimize dependence on any one person. To facilitate communications with vendors, a primary and alternate contact should be designated to handle system problems.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

COMMUNITY FINANCIAL INSTITUTION IS EXAMINATION WORKPROGRAM

Certificate/Charter Number: _____

Name of Financial Institution: _____

Location (City and State): _____

Date of Examination: _____

Examiner In Charge: _____

Assisting Examiner: _____

Assisting Examiner: _____

INSTRUCTIONS

This workprogram should be used with the guidance provided in the *1996 FFIEC IS Examination Handbook.*

Each community financial institution has a unique mixture of Information Systems (IS) with applications processed by in-house systems and/or service bureaus. This workprogram is designed to assist the examiner in the evaluation of IS related internal routine and control procedures for these environments. Typically in-house systems will utilize vendor-supplied software for processing major applications such as deposits, loans, or trust accounts. The software may be supported by the vendor or a third-party contract programmer. If any of the major applications are supported by an internal programming function, the full FFIEC workprogram should be completed, in order to properly evaluate the additional level of risk.

Serviced institutions may have some or all applications processed by a servicer. This can be accomplished by either having the items to be processed sent to the servicer via courier or through a Remote Job Entry (RJE) arrangement. RJE institutions capture their data on-site, electronically transmit the data to a remote servicer for processing, receive (by wire or courier) reports back, and reconcile the output.

The workprogram should be completed and retained in the workpapers with exceptions addressed in the report of examination as appropriate. In those institutions which employ a combination of in-house and servicer processing, certain questions in this workprogram will need to be answered from both perspectives.

Before the start of the examination, the examiner should review the response to the pre-examination letter, if utilized. The examiner should then complete the application checklist to determine which applications are processed in-house or serviced. For institutions with applications processed in-house, determine the method of software support (vendor, contract programmer, or in-house). Review the Shared Application Software Review (SASR), if available. If contract programming is utilized, complete the "Systems Development and Programming" section

of the FFIEC workprogram. A contract programmer is normally a third party, not directly related to the software vendor, who is employed on a periodic or ongoing basis to maintain or enhance the software. Contract programmers can be individuals or corporations. If major applications are supported by in-house programming, the full FFIEC workprogram should be used. For institutions that operate as RJE facilities or are serviced, the servicer's most recent IS examination and/or third-party review (if available) should be reviewed.

The examiner should select one or more applications (DDA, savings, commercial loans, etc.) for review. The purpose of this review is to determine the adequacy of user documentation, appropriateness of transaction controls, and sufficiency of output for completing the “Systems and Programming and Operations” sections of the workprogram. At subsequent examinations, a different application(s) should be reviewed.

The examiner should perform all work steps and answer all applicable questions for the operation under examination. Those questions which are relevant to an in-house system are identified with an "I," while those which pertain to a serviced environment are identified with a "S." Questions which have not been annotated should usually be answered for all systems examined. Questions which do not apply should be answered "N/A."

The workprogram is divided into eight sections, each containing a series of work steps (upper-case) and related questions. Work steps generally reference the related questions. Completion of the work steps should be indicated by the examiner's initials. Each question is worded so that a "yes" answer generally indicates the presence of adequate internal controls. Questions answered "no" do not necessarily indicate a deficiency since compensating controls may exist. Examiners must review for compensating controls and, if found effective, document the controls in the "Comments" section. Generally, all questions that are answered negatively and do not have adequate compensating controls should be brought forward to the "Summary of Exceptions" for discussion with senior management. Due to the varying degree of sophistication in community financial institution IS operations, the examiner may determine that some negative answers do not represent a significant risk in a given operation and need not be brought forward for discussion and/or inclusion in the report findings. This determination should be documented next to the appropriate question.

Each examination should include a review of exceptions from prior examinations, audits/reviews, and follow-up correspondence. Any unresolved exceptions should be included in the "Summary of Exceptions." In addition, management's plans for significant changes that could affect future examinations should be documented in the workprogram and the Report of Examination. The examiner is reminded that this workprogram is a guide for conducting examinations of data processing operations and, if areas of concern not addressed by the workprogram are encountered, it is incumbent upon the examiner to expand the scope of the examination to include a review of those areas. When internal controls appear grossly deficient and little progress toward correction is apparent, the examiner-in-charge should consider utilization of the FFIEC workprogram and Examination Report.

Materials obtained from the data center or developed by the examiner should be included in the workpapers with any other information needed to fully support examination findings. Exhibits which have a continuing significance should be carried forward from the previous examination.

A schedule cross referencing the workprogram questions to the 1996 FFIEC IS Examination Handbook is included at the end of this workprogram. The first item in each column (in bold) refers to work steps or questions in this workprogram. To the right is the chapter number and page reference from the *Handbook* which contains information relating to the issue.

APPLICATIONS CHECKLIST

Certificate/Charter Number: _____
Financial Institution Name: _____
Location: _____

Applications	Software Vendor/Package or Servicer/Processing Site	In-house	Serviced
General Ledger			
Investments			
Loans:			
Commercial			
Construction			
Mortgage			
Home Equity			
Instalment			
Credit Cards			
Student			
Check Credit			
Deposits:			
Demand			
Savings			
Time			
CIF			
Trust			
ATM/POS			
Payroll			
Other			

Instructions: Provide details for vendors and/or servicer. Check the appropriate In-house or Serviced Box.

SUMMARY OF EXCEPTIONS

Summarize deficiencies, management's response and projected date of correction.

SECTION	EXCEPTION	MANAGEMENT'S RESPONSE	DATE OF CORRECTION

1. INTERNAL/EXTERNAL AUDIT

WORKSTEPS

1.1 Review the minutes of the board of directors and the audit or examining committee for comments and actions relating to any audit or "IS" matters and extract pertinent information. (1.4 - 1.7)

1.2 Obtain or prepare a biographical worksheet or resume on internal auditor. (1.8, 1.9)

1.3 Review audit reports (internal and external and reviews since the last examination). Workpapers may be reviewed if deemed necessary. (1.4 - 1.7, 1.10)

RELATED QUESTIONS

1.4 Is an audit of IS related activities performed at least annually?

1.5 Does the auditor routinely submit written reports and audit schedules to the board of directors or the audit committee?

1.6 From the review of audit report(s) since the last examination, indicate, with respect to IS, if the report(s) adequately:
   a. Describes scope and objectives.
   b. Describes deficiencies. If so, list major deficiencies.
   c. Suggests corrective action.
   d. Details follow-up/correction of prior audit or regulatory examination exceptions.

1.7 Does the auditor, designated officer or employee (someone not directly involved in the daily processing activities) periodically review the following:
   a. Segregation of duties – input/processing/output?
   b. Balancing of input and output totals?
   c. Independent proofs of all applications?
   d. Reconcilement of all applications?
   e. Balancing of output totals to the general ledger?
   f. Controls over unposed items?
   g. Controls over supervisor overrides?
   h. Follow-up of exception reports?
   i. Off-premises storage of backup data files, programs, operating system and supporting documentation?
   j. Disaster recovery procedures and backup agreements?
   k. Computer operations?
   l. Physical security?

m. Programming, if applicable?
n. Parameter changes?
o. Installation of emergency changes, and vendor provided program updates and releases?
p. Teleprocessing/networking/data security?
q. Microcomputers and/or networks (e.g. LAN, WAN)?
r. Wire transfer?
s. Automated Clearing House (ACH)?
t. Automated Teller Machines (ATM)?
u. Point of Sale (POSactivities)?
v. Employee accounts?

1.8 Does the auditor (or designee) have any conflicting duties? If so, list.

1.9 Is audit expertise and training sufficient for the complexity of the system and the risk to the institution?

1.10 Is audit software used? (If so, identify program, describe uses, controls, and indicate when last used.)

1.11 Does the auditor provide input for hardware/software purchases? (IS Steering Committee decisions, etc.)

1.12 Carry exceptions forward to "summary of exceptions" schedule.

Examiner | Date
_____|_____

Reviewer's Initials

2. MANAGEMENT

WORKSTEPS

2.1 List management committees which handle IS related matters and provide a brief description of their responsibilities. Review minutes and document significant matters. (2.9, 2.10, 2.11, 2.15)

2.2 If concurrent with other examinations, consult examiners regarding the accuracy, quality, and completeness of reports.

2.3 Summarize any significant plans for changes in management IS personnel, software, hardware or operating procedures.

2.4 Obtain or prepare an organization chart and indicate duties of IS personnel. (2.11 2.12)

2.5 Report generator capabilities allow the financial institution to design and produce custom reports from master file records. Determine if the financial institution has this capability.

2.6 Review contracts for applications processed by servicers see list prepared for work step 3.1. (2.22 - 2.25)

2.7 If institution is serviced, review the most recent regulatory examination and third-party review of the servicer.

2.8 From exceptions noted in this and other sections, assess management and staff ability to adequately resolve the noted deficiencies.

RELATED QUESTIONS

2.9 Are reports produced for senior management, IS management and user departments satisfactory?

2.10 Does senior management annually review IS related policies and procedures and is the review documented?

2.11 Has management taken satisfactory action to correct prior regulatory examination and audit exceptions?

2.12 Is adequate management succession provided?

2.13 Has someone been given overall responsibility for IS security?

2.14 Is there a written IS security policy? If so, does it adequately address all IS areas?

2.15 Does senior management periodically analyze the financial condition and stability of its significant vendor(s) and/or servicer(s)?

2.16 Are procedures in place for requesting reports utilizing the vendor's or servicer's report generator?

2.17 Is access to the query language adequately controlled?

2.18 Are the query instructions used to produce reports using the report generator reviewed by an independent, knowledgeable party?

2.19 For significant software applications, is the institution a member of the vendor's users group?

2.20 Are all capitalized IS costs amortized over a reasonable period of time (generally 4 to 7 years)?

2.21 Are assumptions, data, and calculations used in financial models reviewed for reasonableness by individuals with sufficient expertise and independence?

2.22 As a serviced institution, is each automated application covered by a written contract? If so, does each contract cover:

a. Ownership and confidentiality of files and programs?
b. Liability limits for errors and omissions?
c. Frequency, content, and format of input and output?
d. Fee structure, including:
   (1) Current fees?
   (2) Provisions for changing fees?
   (3) Fees for special requests?
e. Provisions for backup and record protection?
f. Notice required (both parties) for termination of service and the return of customer records in machine readable form?
g. Time schedules for receipt and delivery of work, including processing priorities?
h. Insurance carried by the servicer?
i. Liability for documents in transit?
j. Audit responsibility?

k. Provision to supply the serviced institution with yearly financial statements (preferably audited with both consolidated and unconsolidated figures when applicable)?

2.23 As a serviced institution, is each contract reviewed by legal counsel?

2.24 As a serviced institution, does insurance coverage include the following provisions:
a. Extended blanket bond fidelity coverage to employees of the servicer?
b. Insurance on documents in transit including the cash letter?
c. If the serviced institution is relying on the servicer and/or an independent courier for insurance covered in a and b respectively, is adequate evidence of that coverage on file?

2.25 As a serviced institution, is there an annual re-evaluation of the servicer's performance that includes:
a. Financial condition?
b. Costs?
c. Ability to meet future needs?
d. Quality of service?
e. Control environment at the data center?
f. Emergency backup provisions?
g. Insurance requirements?

2.26 As a serviced institution, does management obtain and review the servicer's internal or external audits, examination reports, and/or third-party reviews? (If yes, detail exceptions and corrective action.)

2.27 Is there annual documented review of insurance coverage? Does this coverage include:
a. Employee fidelity?
b. EDP equipment and facilities?
c. ACH/ATM/POS (EFT) activities?
d. Items in transit?
e. Business interruption?
f. Media reconstruction?
g. Errors and omissions?
h. Extra expense?

2.28 Carry exceptions forward to “summary of exceptions”

Examiner | Date

_____|_____

Reviewer's Initials

3. SYSTEMS AND PROGRAMMING

WORKSTEPS

3.1 Using the application checklist, prepare a schedule for all applications processed in-house or by a servicer. Include, as appropriate, the vendor's or servicer's name, software package name and version number. Review each contract and/or license agreement. (3.5, 3.6)

3.2 For this and all of the following sections, review the shared application software reviews (SASR) for the software vendors listed on the application checklist, if available. (Note: the SASR is an internal regulatory document and is not to be shared with management.)

3.3 Describe procedures for implementing program updates, releases, and changes. (3.7 - 3.10)

3.4 Determine procedures for setting/changing in-house parameters (interest rates, service charges, etc.) (3.11, 3.12)

RELATED QUESTIONS

3.5 Is a software contract or license agreement in effect for all leased software? If so, does it grant the institution:
   a. Possession of current source code and program documentation for each application?
   b. The ability to obtain, use and modify the software in the event the software vendor is unable or unwilling to properly maintain the program(s)?

3.6 If documentation and source code are contractually held under escrow agreement, does the institution have independent assurances that these items are current?

3.7 Are vendor updates, releases, and emergency program changes reported to senior management before implementation or as soon as possible thereafter?

3.8 For remote vendor access to the computer, is there adequate control such as:

a. One-time dial-in password access controlled by the institution?
b. No dial-in access without institutional action (turn on modem, open port, etc.)?
c. Call-back or automated dial-back procedures before vendor access is allowed?
d. Detailed activity log of software and data file access?

3.9 Have all vendor updates and releases been installed? If not, what is the effect on vendor support?

3.10 Is senior management informed of delays in installing program updates and releases?

3.11 Do all in-house parameter changes (interest rates, service charges, etc.) receive prior senior management approval?

3.12 Are parameter change results verified the next day?

3.13 Carry exceptions forward to "summary of exceptions."

Examiner | Date

_____|_____

Reviewer's Initials

4. OPERATIONS

WORKSTEPS

4.1 Using available instructions and observations, chart the flow of a transaction (such as a deposit or loan payment) from initiation through the system to final reconcilement. (4.8 - 4.13)

4.2 Obtain a list of all compilers and utility programs that have data or program altering capabilities. (4.20)

4.3 Obtain or prepare a schedule of major computer equipment. Include manufacturer, model, and main memory size. If equipment is leased, indicate name of lessor, terms of lease, and insurance coverage. (4.21)

4.4 Obtain and verify a list of tapes, disks, documentation, etc., located at the off-premises storage facility. (4.25 - 4.31)

4.5 If the financial institution provides data processing services for nonfinancial institution customers, list the number of customers and the applications processed. (4.46)

RELATED QUESTIONS

4.6 Are adequate and current operator and user instructions provided?

4.7 Do user instructions cover:
   a. Preparation and control of source documents?
   b. Control, format, and usage of output?
   c. Settlement and reconcilement procedures?

4.8 Is separation of duties and responsibilities adequate in the following areas:
   a. Input preparation and balancing?
   b. Data entry?
   c. Operation of the computer system?
   d. Handling of rejects for reentry?
   e. Review and handling of unposed transactions?
   f. Balancing of final output?
   g. Statement preparation?

4.9 Are there adequate input/output controls and reconcilement procedures for the application(s) selected for review? Do they include:
   a. Establishment of dollar and nondollar controls before they are sent for processing?

b. Receipt of all scheduled output reports even when reports contain no activity?
c. Effective review of all output and exception reports?

4.10 Are rejected, unposed, and listings of captured items independently balanced?

4.11 Is it a requirement that master file change requests (such as address changes, due dates, interest rates):
a. Be in writing?
b. Identify the originating personnel?
c. Be reconciled to the change report by an independent individual?

4.12 Are source documents microfilmed or otherwise recorded before being transported to the data center?

4.13 Is all computer output (printouts, microfiche, optical disks, etc.) adequately controlled and disposed of?

4.14 Are negotiable items which are computer processed (CD interest checks, etc.) adequately controlled?

4.15 Is the operation of equipment limited to personnel who do not perform conflicting duties?

4.16 Are adequate safeguards in effect to ensure that only authorized personnel are permitted in the computer area?

4.17 Have an adequate number of financial institution personnel been trained to supervise and operate the system to reduce dependence on key personnel?

4.18 Are data processing duties satisfactorily rotated?

4.19 Are data processing personnel denied access to source programs, program listings, and other documentation that are unnecessary to perform their duties?

4.20 Are compilers and utility programs with data or program altering capabilities adequately controlled by:
a. Dual control procedures after removal from the system?
b. A password system?
c. Other acceptable methods? (Explain)

4.21 a. Is there a maintenance agreement for major EDP equipment?

b. Is the equipment leased and, if so, was it capitalized and booked as an asset of the institution?

4.22 Is a problem log maintained?

4.23 Are management reports (such as manual or machine generated logs, exception reports) adequate to monitor and evaluate IS activities?

4.24 Are exception and management reports adequately reviewed on a timely basis? If so, how is the review documented?

4.25 Is electronic media stored in a fire resistant, limited access, area both in the financial institution and at the backup site?

4.26 Is a copy of all master files taken off-site promptly after updating and not left in the data center overnight or over a weekend?

4.27 In instances where master files are not rotated off-site in a timely manner, is a backup copy of transaction files taken off-site before the update process is initiated?

4.28 Is there adequate and current off-premises storage of:
a. Data files?
b. Source and object programs?
c. System and program documentation?
d. Operating systems and utility programs?
e. Reserve supplies?
f. User and operator instructions?
g. A copy of the contingency plan and backup agreement?

4.29 Is there a current inventory list of the items in question 4.28?

4.30 Is access to on-site and off-site data files (tapes and/or disks) limited to authorized personnel?

4.31 Is the off-site storage facility sufficient distance from the data center so that an event will not normally affect both sites?

4.32 Is the computer area adequately protected by:
a. Heat and smoke detectors?
b. Fire extinguishers?
c. Remotely monitored alarm systems?
d. Other methods? (Explain)

4.33 Is the computer area uncluttered and hazard free?

4.34 Is the data center equipped with an appropriate uninterrupted power supply (UPS)?

4.35 Does the emergency plan adequately provide for:
   a. Personnel evacuation?
   b. Assignment of action to be taken in specific emergencies including the safe storage of data files and documents?
   c. Power-off procedures?
   d. Restart and recovery procedures?

4.36 Are employees familiar with their responsibilities under the emergency plan?

4.37 Does the contingency plan adequately address:
   a. Under what conditions the backup site would be used?
   b. Decision making responsibility for use of the backup site?
   c. Procedures for notification of the backup site?
   d. A checklist of data files, programs, and other items to be transported to the backup site?
   e. Provisions for special forms and backup supplies?
   f. Remote terminal activities?
   g. Processing instructions and priorities?

4.38 Is the contingency plan reviewed annually by the board of directors?

4.39 Has it been conclusively determined that the backup site has sufficient:
   a. Hardware and time to capture all of the institution's daily transactions?
   b. Excess processing time to complete the institution's critical work each day?
   c. Telecommunications facilities?

4.40 Is a comprehensive written agreement in effect with the backup site?

4.41 Is management notified of equipment changes at the backup site?

4.42 Has the contingency plan, including backup site, been tested within the past 12 months using only off-site materials?

4.43 Has a report detailing the scope and results of the backup test been presented to senior management?

4.44 If the institution is serviced, does it subscribe to disaster recovery services offered by the servicer? If not, explain.

4.45 Are the following in place for image capture systems:
   a. Automated journals and audit trails that document access to and modification of images?
   b. Controls to ensure stored images cannot be altered, erased or lost?
   c. Procedures to prevent the destruction of original documents before it is determined that the images are readable?
   d. Procedures to address traditional controls (such as date stamps, control numbers, and review signatures)?
   e. Controls to prevent faulty images, improper indexing, and incomplete or forged documents from being entered into the system?
   f. A backup copy of the image medium stored off-site?
   g. Periodic evaluation of legal issues?

4.46 Are data processing services provided for non-financial institutions? If so:

   a. Are written contracts in effect?
   b. Do the contracts provide adequate protection and establish liability for both the customer and the financial institution?

4.47 Are data processing services provided for other financial institutions? If so, complete the "Customer Service Activities" section of this FFIEC workprogram.

4.48 Carry exceptions forward to "summary of exceptions" schedule.

Examiner | Date

_____|_____

Reviewer's Initials

5. NETWORKING and DATA SECURITY

WORKSTEPS

5.1 Determine the approximate number of terminals. Detail ports and related controls for dial-in access. (5.6, 5.7)

5.2 List processing modes used by the institution (e.g. file maintenance, memo-post, on-line update, inquiry only, etc.).

5.3 Obtain a current listing of all system users and their access capabilities. (5.8 - 5.11)

5.4 Compare a sample of users' access authority with their assigned duties and responsibilities.

5.5 Determine password parameters (length, numeric/alphanumeric, composition, etc.) (5.12)

RELATED QUESTIONS

5.6 Is access to the system restricted by:
- a. Physical terminal locks?
- b. Passwords?
- c. Unique operator identification?
- d. Functions available to specific terminals?
- e. Automatic timeout if left unattended? If so, how long?
- f. Automatic log-off after repeated failed access attempts? If so, how many?
- g. Time of day and day of week?

5.7 Do controls for remote dial-in terminals include:
- a. Senior management approval?
- b. Limiting the activities which can be performed?
- c. Auto call-back to identify dial-in terminals/users?
- d. Other controls similar to 5.5?

5.8 Are passwords:
- a. Changed at an interval appropriate to users' capability? If so, how often?
- b. Suppressed from all output?

5.9 Are all users restricted as to:
- a. What files they can access?
- b. What transactions they can initiate?

5.10 Are user access levels approved and periodically reviewed for appropriateness?

5.11 Are IDs and passwords revoked when users:
   a. Leave the employment of the institution?
   b. Are absent for an extended period of time?

5.12 Do password requirements discourage the use of passwords which can be easily guessed?

5.13 Are reports which record unsuccessful attempts to gain access to the telecommunications system or applications routinely reviewed? If so, how is the review documented?

5.14 Are reports which record activities outside normal business hours produced?

5.15 Is a transaction file maintained for all messages received from all terminals?

5.16 Does the transaction file contain the:
   a. Identity of the user?
   b. Terminal?
   c. Transaction code?
   d. Detail to identify the transaction?
   e. Date and time of the transaction?

5.17 Carry exceptions forward to "summary of exceptions" schedule.

Examiner | Date
_____|_____

Reviewer's Initials

6. RETAIL EFT and ACH

WORKSTEPS

6.1 Obtain or prepare a brief description of ATM and POS services. List network memberships. (6.7)

6.2 Obtain and review contracts for ATM network services and with card vendors, as applicable. (6.7)

6.3 Determine card and personal identification number (PIN) issuance procedures. (6.8 - 6.12)

6.4 Review ATM maintenance and balancing procedures. (6.13 - 6.15)

6.5 Obtain and review ACH customer and POS merchant agreements. (6.16)

6.6 Review ACH procedures. (6.17 - 6.20)

RELATED QUESTIONS

6.7 Are there written contracts with ATM card vendors?

6.8 If the financial institution produces cards in-house:
   a. Are blank cards kept under dual control and accounted for in each step of encoding, embossing, stuffing, and mailing?
   b. Are spoiled cards destroyed under dual control and is the destruction properly documented?

6.9 Are there adequate controls over PIN administration (mailing, issue, and lookup)?

6.10 Are cards and PINs always mailed separately and with a sufficient period of time (usually three days) between mailings?

6.11 Are personnel having custody of cards prohibited from also having PINs?

6.12 Are returned cards controlled and accounted for by individuals other than those with card issuance or system/operations responsibilities?

6.13 Are captured cards adequately controlled?

6.14 Are ATM transactions reconciled daily?

	Comments
6.15 Are security devices and procedures for each ATM adequate?	
6.16 Are there written agreements for all ACH and POS arrangements?	
6.17 Are ACH terminals adequately controlled by passwords and user IDs?	
6.18 Are ACH terminals located in a secure area?	
6.19 Are large item reports and new account reports for ACH activities routinely reviewed?	
6.20 Are ACH activities reconciled daily?	
6.21 Carry exceptions forward to "summary of exceptions" schedule.	

Examiner | Date

_____|_____

Reviewer's Initials

7. END-USER COMPUTING

WORKSTEPS

7.1 Review the institution's microcomputer policy. (7.3)

7.2 Obtain or prepare a list of all microcomputers and determine the applications processed. (7.4 - 7.11)

RELATED QUESTIONS

7.3 Does the microcomputer policy adequately address:
- a. Hardware and software purchases?
- b. Software development?
- c. Security issues?
- d. Control procedures?
- e. Contingency planning?
- f. Use of unauthorized software?
- g. Use of unlicensed software?
- h. Virus protection procedures?
- i. Downloaded data used in PC-based applications?
- j. Adherence to software licensing agreement?

7.4 If microcomputers have access to the mainframe or minicomputer:
- a. Is access controlled via call-back or password procedures?
- b. Are there procedures to ensure the integrity of downloaded data is maintained in further processing?
- c. Are there procedures to control uploading of data?

7.5 Is access to microcomputers adequately controlled during both business and non-business hours?

7.6 Are procedures adequate to provide for separation of duties for origination, input and output reconciliation?

7.7 If a microcomputer is utilized for multiple purposes:
- a. Is there adequate security to limit particular software to authorized users?
- b. If passwords are used, are they properly administered?

7.8 Is electronic media properly controlled and stored?

7.9 Is virus detection software used on all microcomputers?

7.10 Do controls over programs:
- a. Prohibit unauthorized copying?
- b. Ensure program integrity?

7.11 Do microcomputer procedures provide for:
   a. Backup of critical programs and data files?
   b. Appropriate frequency of backup?
   c. Off-site storage, if appropriate?
   d. Employee responsibilities during an emergency?

7.12 Carry exceptions forward to "summary of exceptions" schedule.

Examiner | Date
_____|_____

Reviewer's Initials

8. CLIENT/SERVERS (LANS/WANS)

WORKSTEPS

8.1 Review applications and equipment on the network and determine the overall risk to the institution.

8.2 Obtain and review the policy, written standards, and procedures for network design, support, and security. (8.6)

8.3 Identify the network administrator's duties and responsibilities. (8.8 - 8.10)

8.4 Obtain a current listing of all network users and their access capabilities and rights. (8.17, 8.18, 8.20)

8.5 Review password administration procedures. (8.17 - 8.21, 8.26)

RELATED QUESTIONS

8.6 Does the network policy address:
- a. Approval and purchase of LAN hardware?
- b. Approval of purchase or development of network applications and system software?
- c. Documentation of application and system software?
- d. Data confidentially, integrity, and availability?
- e. Frequency and retention periods for network(s) backup?
- f. Personal use of network resources?
- g. Adherence to software licensing agreements?
- h. Hardware maintenance?
- i. Problem logging/reporting and monitoring?
- j. User responsibilities for security, workstation maintenance, and backup of data files?
- k. Prevention and detection of computer viruses?
- l. Responsibility/accountability for system and data ownership, support and data integration?
- m. Training program availability and usage by staff ?
- n. Inter-platform standards including: data transmission, data sharing, and data transfer.

8.7 Has a network administrator been appointed? If so, is there adequate backup for this position?

8.8 Is the network administrator technically and administratively qualified?

8.9 Do the network administrator's responsibilities include:
- a. Monitoring network efficiency (response time, utilization of disk space, etc.)?
- b. Troubleshooting network problems?

c. Monitoring environmental conditions?
d. Backing up the system, shared data files, and application programs on the file server?
e. Prevention and detection of computer viruses?

8.10 Does the network administrator have any conflicting duties? If so, list.

8.11 Is there a network security officer? If so, do the duties include:
a. Monitoring security violations? (Unauthorized and unsuccessful access attempts)
b. Password administration?

8.12 Is the network software vendor's financial stability periodically reviewed by senior management?

8.13 Do vendor contracts adequately address software support provided, and clearly define hardware maintenance services and costs?

8.14 Is the use of data scopes (devices used to monitor network traffic) adequately restricted?

8.15 Are surge protectors and UPS systems installed as necessary?

8.16 Is physical access to network file servers restricted to authorized personnel?

8.17 Are network passwords and access codes changed periodically and suppressed from all output?

8.18 Are IDs and passwords deleted from the network when users leave the employment of the institution?

8.19 Are passwords encrypted?

8.20 Are there restrictions limiting access to the security tables (e.g. access codes, passwords)?

8.21 Are workstations and/or user access codes automatically disabled after a predetermined number of unsuccessful log-on attempts?

8.22 Is a time-out control in effect to automatically log-off a workstation after a predetermined period of inactivity?

8.23 If the network is connected to an outside source (through modem or dial-up network) do controls include:
a. Senior management approval?
b. Limiting the activities which can be performed?
c. Auto call-back to identify dial-in users?

d. Passwords?
e. Unique operator identification?
f. Automatic log-off after a predetermined number of failed access attempts?

8.24 Is a current version of anti-virus software run automatically on all workstations daily? If not, how often?

8.25 Are critical and/or sensitive network data files and applications identified and adequately protected?

8.26 Are user access levels and rights periodically reviewed for appropriateness?

8.27 Are network activity reports independently reviewed on a regular basis?

8.28 Is there an audit trail documenting all changes made to:
a. Network parameters?
b. Security table(s)?
c. Operating system?

8.29 Is there a source to insure timely replacement of critical network hardware components?

8.30 Is track, disk, or server mirroring used to back up critical data while processing to avoid loss of work during operating hours?

8.31 Are off-site backup data files adequately protected in a secure location?

8.32 Are security tables backed up and rotated to an off-site storage location as needed?

8.33 Is on-site backup of network files kept in a location sufficiently remote from the server?

8.34 Is recovery of critical network applications and data files included in the institution's contingency plan?

8.35 Carry exceptions forward to "summary of exceptions" schedule.

Examiner | Date
_____|_____

Reviewer's Initials

Cross-reference of all community IS workprogram questions to the appropriate section of the 1996 FFIEC IS Examination Handbook. Reference is shown as chapter number followed by page number.

1. INTERNAL/EXTERNAL AUDIT

1.4 - 8-7 & 16.
1.5 - 8-11.
1.6 - 8-3, 11, & 12.
1.7 - 8-7.
1.8 - 8-4 & 5.
1.9 - 8-4.
1.10 - 8-9.
1.11 - 8-10.

2. - MANAGEMENT

2.9 - 9-15.
2.10 - 9-8.
2.11 - 9-14.
2.12 - 9-14.
2.13 - 14-1.
2.14 - 14-1.
2.15 - 9-11, 12-4.
2.16 - 14-12.
2.17 - 14-12.
2.18 - 14-12.
2.19 - 6-16.
2.20 - 22-13.
2.21 - 9-15.
2.22 - 22-9.
2.23 - 22-9.
2.24 - 9-12, 22-6.
2.25 - 22-13 & 15.
2.26 - 22-15.
2.27 - 9-12.

3. - SYSTEMS & PROGRAMMING

3.5 - 16-3 & 8.
3.6 - 16-7.
3.7 - 16-6.
3.8 - 16-5.
3.9 - 23-8.
3.10 - 16-6.
3.11 - 23-7.
3.12 - 23-7.

4. - OPERATIONS

4.6 - 13-1.
4.7 - 13-1.
4.8 - 13-1.
4.9 - 13-12.
4.10 - 13-11.
4.11 - 13-17.
4.12 - 13-15.
4.13 - 13-16.
4.14 - 14-5.
4.15 - 13-6.
4.16 - 14-5.
4.17 - 9-14.
4.18 - 13-1.
4.19 - 13-7.
4.20 - 14-10.
4.21 - 13-2.
4.22 - 13-2.
4.23 - 13-3.
4.24 - 9-8.
4.25 - 13-8.
4.26 - 13-4.
4.27 - 13-4.
4.28 - 13-4.
4.29 - 10-3, 14-6.
4.30 - 14-7.
4.31 - 13-5.
4.32 - 10-5.
4.33 - 10-5.
4.34 - 10-5.
4.35 - 10-5.
4.36 - 10-5.
4.37 - 10-1.
4.38 - 10-1.
4.39 - 10-6.
4.40 - 10-6.
4.41 - 10-6.
4.42 - 10-6.
4.43 - 10-6.
4.44 - 10-6.
4.45 - 17-1.
4.46 - 22-15.

5. NETWORKING/DATA SECURITY

5.6 - 14-8.
5.7 - 14-8.
5.8 - 14-8.
5.9 - 14-8.
5.10 - 14-8.
5.11 - 14-8.
5.12 - 14-8.
5.13 - 14-8.
5.14 - 14-13.
5.15 - 14-9.
5.16 - 14-9.

6. - RETAIL EFT and ACH

6.7 - 20-5.
6.8 - 20-6.
6.9 - 20-4.
6.10 - 20-4.
6.11 - 20-4.
6.12 - 20-5.
6.13 - 20-4.
6.14 - 20-4.
6.15 - 20-4.
6.16 - 21-1
6.17 - 21-2
6.18 - 21-2
6.19 - 21-2
6.20 - 18-7

7. - END USER COMPUTING

7.3 - 16-3.
7.4 - 14-13, 16-1.
7.5 - 16-5.
7.6 - 16-8.
7.7 - 14-8, 16-5.
7.8 - 14-6.
7.9 - 14-16.
7.10 - 14-7.
7.11 - 14-6, 16-4.

8. - CLIENT/SERVERS (LANS and WANS)

8.6 - 12-2, 16-3.
8.7 - 14-1.
8.8 - 14-1
8.9 - 15-11.
8.10 - 14-12, 15-13 & 15.
8.11 - 14-8.
8.12 - 9-10.
8.13 - 22-9.
8.14 - 15-10.
8.15 - 14-4.
8.16 - 14-4.
8.17 - 14-8.
8.18 - 14-8.
8.19 - 14-8 & 10.
8.20 - 14-9.
8.21 - 14-9.
8.22 - 14-9.
8.23 - 14-14.
8.24 - 14-16.

8.25 - 13-5.
8.26 - 14-1.
8.27 - 15-19.
8.28 - 14-8.
8.29 - 15-9.
8.30 - 13-5.
8.31 - 13-5.
8.32 - 14-8.
8.33 - 13-5.
8.34 - 10-3