

# 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.

<b>SECTION</b>	<b>EXCEPTION</b>	<b>MANAGEMENT'S RESPONSE</b>	<b>DATE OF CORRECTION</b>
----------------	------------------	------------------------------	---------------------------

## 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 reconciliation. (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 reconciliation 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 reconciliation 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?

- 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 confidentiality, 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.

<b>1. INTERNAL/EXTERNAL AUDIT</b>	<b>4.11</b> - 13-17.	<b>6. - RETAIL EFT and ACH</b>
<b>1.4</b> - 8-7 & 16.	<b>4.12</b> - 13-15.	<b>6.7</b> - 20-5.
<b>1.5</b> - 8-11.	<b>4.13</b> - 13-16.	<b>6.8</b> - 20-6.
<b>1.6</b> - 8-3, 11, & 12.	<b>4.14</b> - 14-5.	<b>6.9</b> - 20-4.
<b>1.7</b> - 8-7.	<b>4.15</b> - 13-6.	<b>6.10</b> - 20-4.
<b>1.8</b> - 8-4 & 5.	<b>4.16</b> - 14-5.	<b>6.11</b> - 20-4.
<b>1.9</b> - 8-4.	<b>4.17</b> - 9-14.	<b>6.12</b> - 20-5.
<b>1.10</b> - 8-9.	<b>4.18</b> - 13-1.	<b>6.13</b> - 20-4.
<b>1.11</b> - 8-10.	<b>4.19</b> - 13-7.	<b>6.14</b> - 20-4.
	<b>4.20</b> - 14-10.	<b>6.15</b> - 20-4.
<b>2. - MANAGEMENT</b>	<b>4.21</b> - 13-2.	<b>6.16</b> - 21-1
	<b>4.22</b> - 13-2.	<b>6.17</b> - 21-2
<b>2.9</b> - 9-15.	<b>4.23</b> - 13-3.	<b>6.18</b> - 21-2
<b>2.10</b> - 9-8.	<b>4.24</b> - 9-8.	<b>6.19</b> - 21-2
<b>2.11</b> - 9-14.	<b>4.25</b> - 13-8.	<b>6.20</b> - 18-7
<b>2.12</b> - 9-14.	<b>4.26</b> - 13-4.	
<b>2.13</b> - 14-1.	<b>4.27</b> - 13-4.	<b>7. - END USER</b>
<b>2.14</b> - 14-1.	<b>4.28</b> - 13-4.	<b>COMPUTING</b>
<b>2.15</b> - 9-11, 12-4.	<b>4.29</b> - 10-3, 14-6.	
<b>2.16</b> - 14-12.	<b>4.30</b> - 14-7.	<b>7.3</b> - 16-3.
<b>2.17</b> - 14-12.	<b>4.31</b> - 13-5.	<b>7.4</b> - 14-13, 16-1.
<b>2.18</b> - 14-12.	<b>4.32</b> - 10-5.	<b>7.5</b> - 16-5.
<b>2.19</b> - 6-16.	<b>4.33</b> - 10-5.	<b>7.6</b> - 16-8.
<b>2.20</b> - 22-13.	<b>4.34</b> - 10-5.	<b>7.7</b> - 14-8, 16-5.
<b>2.21</b> - 9-15.	<b>4.35</b> - 10-5.	<b>7.8</b> - 14-6.
<b>2.22</b> - 22-9.	<b>4.36</b> - 10-5.	<b>7.9</b> - 14-16.
<b>2.23</b> - 22-9.	<b>4.37</b> - 10-1.	<b>7.10</b> - 14-7.
<b>2.24</b> - 9-12, 22-6.	<b>4.38</b> - 10-1.	<b>7.11</b> - 14-6, 16-4.
<b>2.25</b> - 22-13 & 15.	<b>4.39</b> - 10-6.	
<b>2.26</b> - 22-15.	<b>4.40</b> - 10-6.	<b>8. - CLIENT/SERVERS</b>
<b>2.27</b> - 9-12.	<b>4.41</b> - 10-6.	<b>(LANS and WANS)</b>
	<b>4.42</b> - 10-6.	
<b>3. - SYSTEMS &amp; PROGRAMMING</b>	<b>4.43</b> - 10-6.	<b>8.6</b> - 12-2, 16-3.
	<b>4.44</b> - 10-6.	<b>8.7</b> - 14-1.
<b>3.5</b> - 16-3 & 8.	<b>4.45</b> - 17-1.	<b>8.8</b> - 14-1
<b>3.6</b> - 16-7.	<b>4.46</b> - 22-15.	<b>8.9</b> - 15-11.
<b>3.7</b> - 16-6.		<b>8.10</b> - 14-12, 15-13 & 15.
<b>3.8</b> - 16-5.	<b>5. NETWORKING/DATA SECURITY</b>	<b>8.11</b> - 14-8.
<b>3.9</b> - 23-8.	<b>5.6</b> - 14-8.	<b>8.12</b> - 9-10.
<b>3.10</b> - 16-6.	<b>5.7</b> - 14-8.	<b>8.13</b> - 22-9.
<b>3.11</b> - 23-7.	<b>5.8</b> - 14-8.	<b>8.14</b> - 15-10.
<b>3.12</b> - 23-7.	<b>5.9</b> - 14-8.	<b>8.15</b> - 14-4.
	<b>5.10</b> - 14-8.	<b>8.16</b> - 14-4.
<b>4. - OPERATIONS</b>	<b>5.11</b> - 14-8.	<b>8.17</b> - 14-8.
	<b>5.12</b> - 14-8.	<b>8.18</b> - 14-8.
<b>4.6</b> - 13-1.	<b>5.13</b> - 14-8.	<b>8.19</b> - 14-8 & 10.
<b>4.7</b> - 13-1.	<b>5.14</b> - 14-13.	<b>8.20</b> - 14-9.
<b>4.8</b> - 13-1.	<b>5.15</b> - 14-9.	<b>8.21</b> - 14-9.
<b>4.9</b> - 13-12.	<b>5.16</b> - 14-9.	<b>8.22</b> - 14-9.
<b>4.10</b> - 13-11.		<b>8.23</b> - 14-14.
		<b>8.24</b> - 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