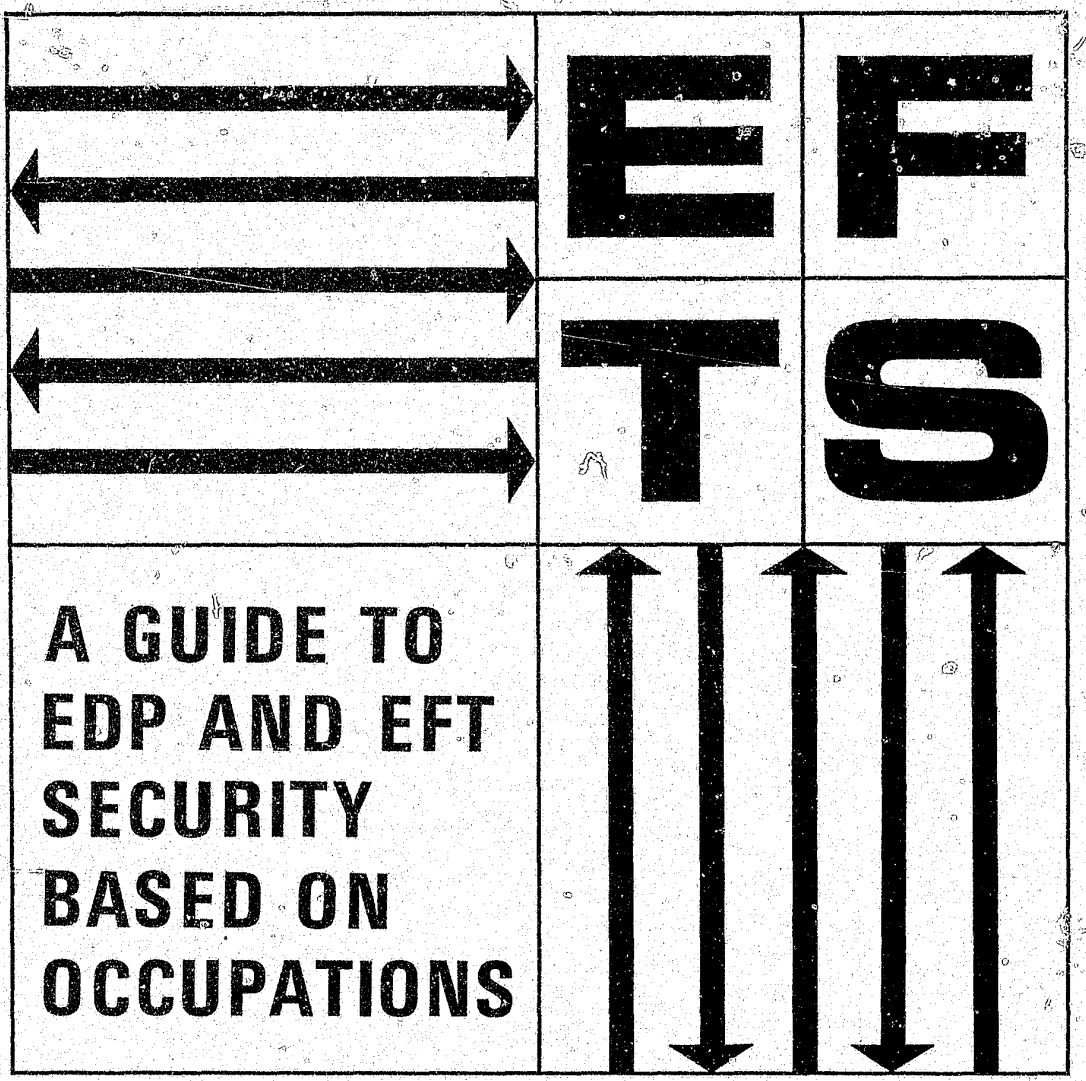
FDIC

Prepared by Division of Management Systems and Financial Statistics, Federal Deposit Insurance Corporation, Washington, D.C. 20429



A GUIDE TO EDP AND EFT SECURITY BASED ON OCCUPATIONS

A GUIDE TO
EDP AND EFT SECURITY
BASED ON OCCUPATIONS

NOVEMBER 1977

Prepared by:
Division of Management Systems
and Financial Statistics
Federal Deposit Insurance Corporation
Washington, D.C. 20429

Consultants: Don B. Parker and
Russell Dewey
SRI International

TABLE OF CONTENTS

I INTRODUCTION

Purpose – This guide is part of a set of papers on the subject of Electronic Funds Transfer (EFT).* The primary purpose of this guide is to supply all people charged with the safe use of EDP (whether in traditional financial institutions or in EFT) with a means of more effectively providing for and evaluating EDP and data communications security from the source of vulnerabilities – people in EFT and banking related EDP occupations.

Losses are growing from accidental and intentional acts involving computers and data communications in financial institutions. Current estimated losses from credit card fraud alone are $500 million and could rise to $6-10 billion by 1986 (Frost and Sullivan, as reported in *Bank Systems and Equipment Journal,* June 1977). Of even greater concern is the growing potential for single instances of massive loss through EFT. As EFT grows, participants will become highly dependent on continuously available computer services in which most of their assets are stored in electronic form. Fortunately, the use of automated systems offers a great potential for prevention, effective detection, and recovery from such losses. This guide describes ways to put that potential to use.

Losses, whether intentional or accidental, can only be caused by two sources: natural events (such as storms) or people. This guide focuses on the people who have the skills, knowledge, and necessary access to cause material losses. Examiners, certified public accountants, internal auditors, security specialists, and line managers need to understand the vulnerabilities caused by various groups of people. This understanding is essential in providing adequate security from losses. To meet that objective, this guide identifies most of these groups, describes the related vulnerabilities, and offers advice on protection.

The principal section of this guide, Occupation Vulnerabilities (Section VIII), contains a vulnerability analysis and two-page description of each of twenty EDP related occupations in financial institutions and EFT. Each description includes the following information:

- job functions
- probable EFT employers
- knowledge, skills, and work area access needed in the occupation related to the position of trust
- vulnerabilities of an EDP system related to accidental and intentional acts that might be perpetrated by an individual in this position
- audit tools and techniques and EDP controls which could reduce the identified vulnerabilities
- conclusion, including issues and problems concerning the vulnerabilities and remedies

Other sections of this guide provide the following:

- a summary for executives (Section II)
- a description of the EDP and EFT environment (Section III)
- general remedies which apply to EDP and EFT personnel (Section IV)
- classification of vulnerabilities (Section V)
- descriptions of applicable EDP audit tools and techniques (Section VI)
- descriptions of EDP controls (Section VII)
- concluding recommendations (Section IX)

Tables are included throughout the guide which cross-refer occupations with remedies.

Limitations – No guide on vulnerability and security can completely and directly apply to each EDP organization. Variations in job descriptions, system configurations, organizations, environments, and procedures require adaptation of the information and advice presented. The occupations included are based on a depiction of the EDP and EFT environments described in this guide (Section III). The vulnerabilities (Section V) are based on four classes: physical, transactional, programming, and electronic. The audit tools and techniques and the EDP controls (Sections VI and VII) were selected from the Institute of Internal Auditors *Systems Auditability and Control* reports (1977), which describe the current state of the art of EDP auditing.

If the observed practices among EFT participant organizations differ from those prescribed in this guide, the guide users should not immediately assume they have found weaknesses in the organization. As there are few standards or generally accepted practices in the computer field, many variations and deviations from descriptions and statements in this guide will be found. When different practices occur, the guide user should consider the factors of the particular situation. The different practices may be as beneficial as the practices recommended in this guide.

Applicability to Small Organizations – The small EFT merchant or financial institution has serious vulnerabilities and often more difficult protection problems than the large organization. Although the small organization has the same exposure as the large organization, it has less resources to devote to security. Assuming a network is only as safe as its

*Other publications in the series are listed on the last page of this guide.

weakest link, the exposure of the small EFT merchant or institution adds to the exposure of other EFT participants in the same network. Larger network participants may resist interfacing their electronic functions with those of smaller EFT participants until certain standards are met.

II EXECUTIVE SUMMARY

This guide was written to help ensure the safe use of computer and data communications technology. It was designed for bank examiners who evaluate audit effectiveness, for auditors who evaluate computer systems and networks security, and for EDP managers who are responsible for the performance of their employees.

Guides to electronic data processing security are usually organized by such functional topics as computer operations, data communications, data preparation, and programming. Another form of presentation is by technical, operational, procedural and physical protection. This guide is different. It is problem oriented, focusing on the vulnerabilities presented by people who can cause losses in EDP, especially in the new use of computers for Electronic Funds Transfer.

Twenty occupations have been chosen based on the skills, knowledge and access to computer services and assets found in EDP and EFT. The occupations and the vulnerabilities each represents from accidental and intentional acts are described in this guide.

Effective security is based on constraining people from causing losses by applying safeguards and controls according to their skills, knowledge and access. This guide helps achieve this goal for each occupation by identifying known controls and audit tools and techniques currently in use according to a set of state-of-the-art reports, *Systems Auditability and Control,* produced for the Institute of Internal Auditors by SRI International. This approach to security has also resulted in identifying the occupations representing the greatest vulnerabilities and the security limitations when dealing with them.

Four classes of vulnerabilities (physical, transactional, programming, and electronic), 17 types of audit tools and techniques for detection, and eight classes of controls for detection and prevention have each been tabulated and their applicability measured for each of the 20 occupations. Also, four basic management actions are described that can increase the trustworthiness and reliability of all EDP employees.

The guide identifies the occupations of greatest trust and for which the least number of controls and audit tools and techniques are effective: facilities engineers, security officers, EDP auditors, application and systems programmers, systems engineers, and programming managers. Controls that affect the widest range of occupations are those that constrain procedural activities among EDP personnel. A need is shown for new and more effective controls for acts that can be perpetrated by programmers and engineers. Only computer center controls and application system development controls were found to effectively apply to programming and electronic classes of vulnerabilities. Few apply to transaction and physical vulnerabilities.

We face a problem today with the advancing use of computer technology and EFT systems in which data worth billions of dollars are stored and processed in computer and data communications systems vulnerable to error prone and unscrupulous people. If these assets were in physical form, they would be stored in time-locked vaults and would be processed and moved under the watchful eyes of guards. The needs of automation preclude this type of safeguarding, yet we do not know how to provide equivalent protection in automated systems, nor are enough resources being expended to develop the needed controls and audit tools and techniques. Fortunately, the potential for sufficient protection at reasonable cost does exist in the use of computers. It remains for us to take advantage of it.

III THE EDP AND EFT ENVIRONMENT

The number of financial terminals being installed in remote locations to automate all or part of the transfer of credits and debits is increasing. SRI International estimates that by 1980 there may be over 100,000 terminals providing a variety of EFT services, including:

deposits
withdrawals
transfers of balances between accounts
direct debits for purchases
balance inquiries
check authorization and guarantee
credit card authorization and data capture
corporate cash management
funds concentration
corporation-to-corporation wire transfers
others

During the last few years, components of this new technology have begun to be implemented in a variety of different configurations, including shared access networks. A shared access network is one which allows the switching of EFT transactions to more than one possible destination regardless of ownership considerations. Because this environment is more complex than single institution dedicated EFT, this guide concentrates on shared access networks.

The principal components of such shared access networks are illustrated in Figure 1.

(1) **Transaction and Programming Terminals** – The terminal (e.g., Automated Teller Machine (ATM), check guarantee terminal cash management terminal) may be operated entirely by one person. It may also be operated by an intermediary, such as a financial institution teller or merchant sales person. The programming terminal provides programmer access to the system.

(2) **Communication Options** – The terminal may be connected to a computer located at a merchant, corporation, or government facility. In this case, the originating computer must be connected to the destination computer through intermediate computers and telephone communication facilities. Figure 1 illustrates the options available to construct such an interconnection. Depending on the complexity of the local environment, the number of institutions participating, and the economic considerations, the terminal may optionally be connected directly to a local financial institution, directly to a joint venture shared EFT switch or (through common carrier facilities) directly to the destination.

(3) **On-Line and Off-Line Files** – EFT files take several forms and may be found in several discreet locations:

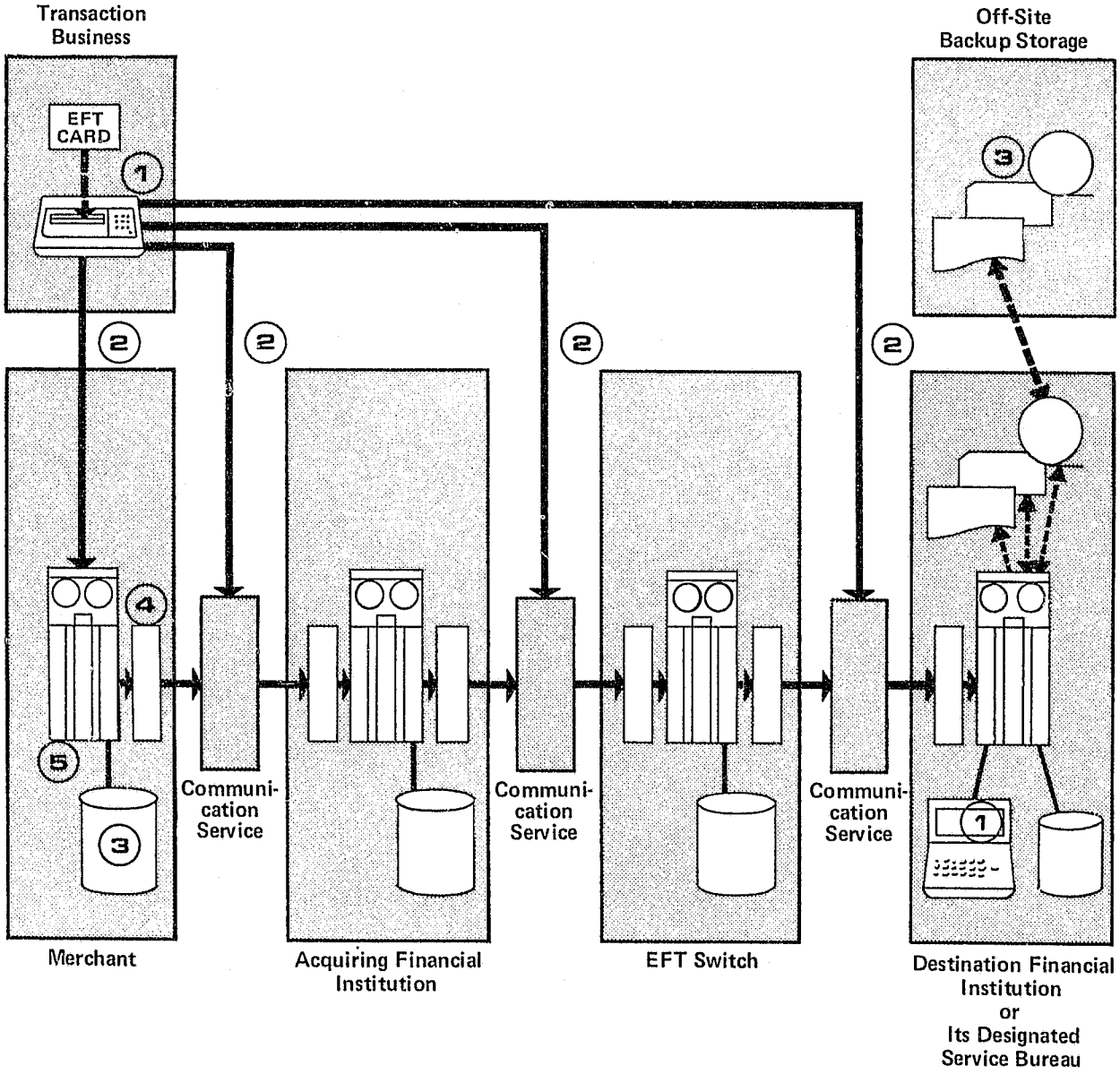
- **At the remote operator** (merchant, corporation, government agency) there may be audit trails of EFT transactions passing through or decision parameters to control the processing of transactions when the remainder of the network is down. There are probably no balances, account or financial institution programs.
- **At the acquiring financial institution** there may not only be audit trails but also balances and account data for its merchants and corporate customers (and for transactions that do not need to be switched, such as an 'on-us' debit.) The acquiring financial institution may also have decision parameters to control the processing of 'not-on-us' transactions when the remainder of the network is down.
- **At the EFT switch** there may be audit trails and decision parameters for any destination facility that may be down. There are probably no financial files other than reconciliation totals and settlement amounts between institutions.
- **At the destination financial institution** there may be audit trails, memo-post master file balances, transaction files with backup, and off-line master files with backup.

(4) **Communication Equipment** – Each computer site will have specialized hardware to interface the EDP system with the external communication lines.

(5) **EFT Hardware and Software** – Each computer expected to participate in such an EFT network must have specialized programs developed. These include:

- terminal protocols
- message format conversions
- switching and routing logic
- interface logic/protocol to other computers
- interface to existing financial software, such as
  - demand deposit accounting
  - savings account accounting
  - customer information data base
  - new account processing

EFT NETWORK



Principal Components

1. Transaction or Programming Terminal
2. Communications Options
3. On-Line or Off-Line Files
4. Communication Equipment
5. Hardware and Software

Electronic Movement

Physical Movement

Figure 1

(6) **Personnel** (Not shown on Figure 1) — The EFT environment is also marked by the diversity and complexity of human skills, knowledge, and access necessary for its operation. These occupations, fully described in Section VIII, also have the potential of causing significant losses to the financial institutions involved through either intentional or accidental actions. Such potential for loss is the primary reason for this guide. Brief summaries of the twenty occupations described in Section VIII are provided below. For more detailed information, the user of this guide should refer to the alphabetized page listing of occupations (p.), which directs the user to the two-page description of each occupation.

Transaction Terminal Operator (merchant clerk, bank teller or consumer) — Keys into a terminal to initiate an EFT transaction.

Computer Operator — By means of the CPU console terminal, directs the execution of tasks within the EDP system, including scheduling, setting priorities, and making updates to the system tables.

Peripheral Equipment Operator — Mounts, unmounts tapes and disks containing master files and other data. Also enters jobs, data, and utility execution cards through the system card reader.

Job Set-Up Clerk — Determines when each job is to be run, how often, and if it needs to be rerun. Causes jobs and data to be entered into the job scheduling queue.

Data Entry and Update Clerk — Causes changes to direct access file data or causes changes to mag tape data by means of either terminal entries or unit record (batch) entries.

Communication Operator — Operates concentrators, multiplexors, modems, line switching units, and similar equipment within the EDP center.

Media Librarian — Stores, preserves, and retrieves data stored off-line (either on magnetic tape, disk, floppy disk, cylinders, or similar media).

Systems Programmer — Writes, debugs, and installs usually resident machine instructions relating to the execution of compilers, utilities, operating system software, communication monitors, data base management software, and other common software not directed at a specific application.

Application Programmer — Writes, debugs, and installs usually non-resident machine instructions relating to the execution of logic to control the processing of a particular application. Causes current version of application program to replace earlier version.

EFT Terminal Engineer, Computer System Engineer, Communication Engineer — Diagnoses hardware failures, isolates faculty components, and repairs or replaces hardware to restore the system to operational status. Usually specializes to the point of transaction terminals (that may have cash stored inside), EDP hardware, and communication equipment. Maintenance and repair may be performed by the original vendor or by one or more firms that specialize in this service.

Facilities Engineer — Inspects, adjusts, repairs, modifies or replaces equipment supporting computer and terminal facilities such as air conditioning, power, lights, heat and water.

Communication Network Manager — Controls the configuration of the communication network through a terminal, placing lines and terminals into/out of service, establishing alternate paths, and starting/stopping polling.

Operations Manager — Manages the operation of computers, peripheral equipment, job control, console operators (peripheral operators - mount/demount files), communication operators and off-line data custodians, and the repair of EDP hardware.

Data Base Manager — Manages the data base files and update technicians.

Programming Manager — Manages the systems development function and application programmers.

Identification Control Clerk — Assigns account numbers, issues PINs, monitors the manufacture, encoding/embossing, and mailing of EFT plastic cards, monitors microfilm paper audit trails, and logs jobs into/out of the EDP center.

Security Officer — Controls the access to and safe use of the EDP systems equipment, libraries, documentation, and other records.

EDP Auditor — Reviews the adequacy of accounting, financial, and operational controls. Monitors compliance with standards and policies and appraises the integrity of data processed through EDP.

The employers for each of the twenty occupations are identified in Figure 2, Occupations by Employers.

OCCUPATIONS BY EMPLOYERS

Occupations	Employers								
	Merchant	Financial Institution	EFTS Switch	FM Contractor	Service Bureau	Telephone Company	Maintenance Vendor	Product Vendor	External Audit Examiner
Operations									
Transaction Operator	X	X	X	X	X		X		
Computer Operator	X	X	X	X	X				
Peripheral Equipment Operator	X	X	X	X	X				
Job Set-Up Clerk	X	X	X	X	X				
Data Entry and Update Clerk	X	X	X	X	X				
Communications Operator	X	X	X	X	X	X	X	X	
Media Librarian	X	X	X	X	X				
Software									
System Programmer	X	X	X	X	X		X	X	
Application Programmer	X	X	X	X	X		X	X	
Hardware									
Terminal Engineer						X	X	X	
System Engineer							X	X	
Communication Engineer						X	X	X	
Facilities Engineer	X	X	X	X	X		X	X	
Management									
Network Manager		X	X	X	X				
Operations Manager	X	X	X	X	X				
Data Base Manager		X	X	X	X				
Programming Manager	X	X	X	X	X				
Other									
Identification Clerk		X			X				
Security Officer	X	X	X	X	X	X			
EDP Auditor	X	X	X		X				X

Figure 2

IV BASIC SECURITY MEASURES

EDP security is primarily a people-oriented matter. Security requires such technical controls as physical access control, personal identification verification, transaction validation, and encryption protection for data communication. Even if such controls are used, none of them are effective unless the people who develop, maintain, use, and are constrained by them are generally trustworthy and motivated to make them work.

Specific controls and audit tools and techniques are identified in this guide for each EDP occupation, but a number of measures are applicable to all personnel engaged in EDP work. These measures are described below:

(1) **Example of Management** — Management in its leadership role sets the goals, standards, and policies of the organization. Subordinates are highly sensitive to management attitude and interest and know when a position taken by management is real or only 'lip service.' This is particularly true in matters of safety of the organization and integrity and honesty of actions. Management of all participant EFT organizations must show dedication and support for the security of the entire network. This includes establishing and subscribing to written policy and procedures, demonstrating a willingness to devote adequate resources to security, delegating sufficient authority and responsibility to auditors and security officers, and supporting all security practices with enthusiasm in ways visible to employees. For example, executives should wear appropriate badges and respect access controls when entering controlled areas. They should conform to policy regarding visitors. They should attend briefings and planning meetings concerning security and refer security matters to the appropriate staff.

(2) **Ethics and Trust** — All managers and employees must be made aware of the requirements for ethical behavior and the importance of their positions of trust. Codes of ethics and sanctions for violation should be established in EDP organizations and prominently displayed and disseminated. Management should support codes and sanctions promulgated by certification organizations, professional societies, and unions that include employees as members. Additionally, each manager and employee should have a clear understanding of his or her position of trust. This should be explained at the time of initial employment, during employment as part of salary and performance reviews, and at termination. If a manager or employee is asked by an auditor or examiner about their positions of trust, they should be able to respond readily, accurately, and fully about the organization's policy and all regulations and laws established for the industry. This interrogation should be part of the audit and examination procedure.

(3) **Periodic Briefings and Training** — All employees should be required to undergo periodic briefings and review of security policy and practice. At the conclusion, each should sign a statement of compliance. The briefings should be interesting and intellectually stimulating. Case studies can be a valuable aid in presentations.

(4) **Background Investigation** — All EDP employees in positions of trust should be required to submit to investigations of their past and current personal lives. The scope and depth of investigation should be stated explicitly and agreed to by all parties before being carried out. The extent of such investigations should be different for the various occupations and consistent with the degrees of trust. The privacy of individuals must be respected as much as possible, but employees must accept the need that certain information be known by their employer. The employer must also ensure confidentiality and proper information gathering procedures consistent with good privacy practices, regulations, and laws. Investigations must be performed before hiring, periodically during employment, and at termination. It is appropriate that each employee's banking, loan, and other major financial practices be known. This may be facilitated by requiring that all financial, retail, and service businesses reveal significant transactions involving the employee. EFT advances should make this increasingly feasible and economical.

(5) **Accountability** — Each aspect of security must be the responsibility of explicitly identified personnel. For each safeguard, control, and level of security management, an individual must be identifiable whose job performance depends on its proper function and effectiveness. One of the responsibilities of management and the auditors is to ensure that this is so.

(6) **Personal Assistance for Personnel** — One of the most frequent motivations for embezzle-

ment in financial institutions is the employee's personal problems. As organized criminal elements and foreign powers gain interest in compromising EFT, coercion of EFT technologists in positions of trust is anticipated. Employees can be insulated from such coercion if they have confidential and legitimate sources of personal assistance. EFT participant organizations should have the resources to supply such help. They should supply specialized, easily available personal financial and advisory services and drug and alcohol rehabilitation programs. In some cases this might be supplied by independent organizations rather than directly by the employer to ensure confidentiality. Employees should have the feeling that they have a confidential source of help for whatever personal problems they may have. This represents a significant means of deterring unauthorized acts and violations of trust.

(7) **Auditability of EDP and Data Communications** – The audit function is the most powerful means for management to ensure the safe use of computer and data communication technology. Two important aspects needing greater attention today are technical competency of auditors and auditability of EDP and data communications activities. Top management must know that auditors understand and are involved in each new system or technical advance being planned. Auditability should be an integral characteristic of each system or technical advance. Among several factors, this requires that audit personnel are assigned to the planning activities, vulnerabilities analysis is performed, adequate controls are specified and properly instrumented for audit review, and that facilities for use of audit tools and techniques are provided.

(8) **Documentation of Security Policies and Procedures** – All policies and procedures regarding security, employee responsibility, and commitment to security should be thoroughly documented, periodically reviewed, and kept current. Additionally, each part of the documentation pertaining to an individual employee should be readily available to him or her. Security documentation in which the employee is not involved should *not* be available to the employee. Auditors should periodically review the documentation and its administration.

In summary, much can be done to create an environment in EDP and EFT organizations in which practical and effective security can be maintained, regardless of the size or complexity of the organization. The security of an EDP system is no stronger than the weakest or most vulnerable employee in a position of trust. Achieving adequate system security requires that it be placed and operated in a secure environment by trustworthy personnel.

V CLASSES OF VULNERABILITIES

Vulnerabilities of EDP to losses from accidental and intentional acts take many forms, limited only by the foibles and ingenuity of people. Four general classes of vulnerabilities associated with computers and data communications have been arbitrarily established. They relate to the skills, knowledge, and access of people in EDP occupations and the remedies of using audit tools and techniques and controls:

CLASS I - Physical: Physical acts include destructive attacks on equipment data and programs, false data entry into computer systems through normal manual input methods, and scavenging for information available in physical form (such as computer output listings, punch cards, reels of tape, and disk packs). Skills needed are minimal. They include physical strength, persuasion in dealing with people, and (possibly) keyboard operation ability. Knowledge is required of the target and its environment and the operational procedures of the EDP staff.

CLASS II - Transactional: Transactional acts include impostering (assuming the identity and privilege of another person) and piggybacking to obtain the same privilege of another person having access rights to a system. This may be done either physically or logically, through terminal and utility program usage to modify, copy, or delete data stored in computer storage media. Skills required include terminal and computer operation knowledge, persuasion in dealing with people, and impersonation of others. Knowledge of interactive and physical access protocols, data file organization, or utility program operation in a particular computer system would also be required.

CLASS III - Programming: This requires more sophisticated skills and knowledge. Various programming techniques can be used such as Trojan Horse attacks, use of trap doors, asynchronous processing attacks, salami techniques (such as round down accumulation), data leakage, the use of logic bombs, and the use of the computer as a tool for simulations and modeling of crimes. These methods can be used in application programs or operating systems and data communications. Skills required include programming and systems analysis. Detailed knowledge is needed of particular application, system, and communication programs. Knowledge of simulation and modeling methods would also be useful.

CLASS IV - Electronic: This class includes wire tapping and electronic hardware modifications to produce the same results as software modification and use. Skills required include electronic fabrication, circuit diagram reading, and electronic tools usage. Knowledge needed includes electronic engineering, digital logic design, and electronic details of specific computers.

Occupations, audit tools and techniques, and controls associated with each class of vulnerability are identified in the following diagrams.

VULNERABILITIES BY OCCUPATION

Occupations*	Vulnerability Classes			
	Class I – Physical	Class II – Transactional	Class III – Programming	Class IV – Electronics
Operations				
Transaction Operator	X	X		
Computer Operator	X	X		
Peripheral Equipment Operator	X	X		
Job Set-Up Clerk	X	X		
Data Entry & Update Clerk	X	X		
Communications Operator	X	X		X
Media Librarian	X			
Software				
System Programmer	X	X	X	
Application Programmer	X	X	X	
Hardware				
Terminal Engineer	X	X	X	X
System Engineer	X	X	X	X
Communication Engineer	X			X
Facilities Engineer	X			
Management				
Network Manager	X		X	X
Operations Manager	X		X	X
Data Base Manager	X	X		
Programming Manager	X	X	X	
Other				
Identification Clerk	X			
Security Officer	X	X	X	X
EDP Auditor	X	X	X	X

*Refer to page listing of Occupation Descriptions (p. 37) for more detailed information.

Figure 3

VULNERABILITIES BY EDP CONTROLS AND AUDIT TOOLS AND TECHNIQUES

Controls and Audit Tools/Techniques	Vulnerability Classes			
	Class I – Physical	Class II – Transactional	Class III – Programming	Class IV – Electronics
Controls				
Transactions Origination	X			
Transactions Entry	X	X		
Data Communication	X	X		
Computer Processing		X		
Data Storage and Retrieval	X		X	X
Output Processing	X	X		
Computer Center	X		X	X
Application System Development			X	
Audit Tools and Techniques				
Test Data Method			X	X
Base Case System Evaluation			X	X
Integrated Test Facility			X	X
Parallel Simulation	X	X	X	X
Transaction Selection		X	X	
Embedded Audit Data Collection		X		X
Extended Records		X	X	X
Generalized Audit Software		X	X	X
Snapshot			X	X
Tracing			X	X
Mapping			X	
Control Flowcharting			X	
Job Accounting Data Analysis	X	X	X	
System Development Life Cycle			X	
System Acceptance and Control			X	X
Code Comparison			X	X
Disaster Testing	X	X		X

Figure 4

VI EDP AUDIT TOOLS AND TECHNIQUES

Introduction – Occupations as sources of vulnerabilities that may be detected by 17 EDP audit tools and techniques are presented in the following table, EDP Audit Tools and Techniques by Occupation Applicability (Figure 5).

The numbers in the entries indicate the degree of applicability. The tools and techniques related to data integrity apply principally to computer operations staff. Tools and techniques related to computer program integrity apply to software and hardware development and maintenance functions. None apply to security officer and EDP auditors since they are the users of the tools and techniques.

The number of applicable tools and techniques is greatest for the more technical and professional occupations and least for clerical and technician occupations. The products of the clerical and technical occupations tend to be more directly observable; therefore, more manual detection techniques apply.

Ranking of Occupations by Number of Applicable Tools and Techniques –

Number of Applicable Tools and Controls	Occupations
14	Applications programmer, programming manager
13	Systems programmer
12	Systems engineer, communications engineer, network manager, operations manager
9	Peripheral operator, terminal engineer
8	Computer operator, communications operator, data base manager
6	Transaction operator, job set-up clerk, identification control clerk
4	Data entry and update clerk
3	Media librarian
1	Facilities engineer
0	Security officer, EDP auditor

EDP AUDIT TOOLS AND TECHNIQUES BY OCCUPATION APPLICABILITY

Occupations	EDP Audit Tools/Techniques for Detection																
	Test Data Method	Base Case System Evaluation	Integrated Test Facility	Parallel Simulation	Transaction Selection	Embedded Audit Data Collection	Extended Records	Generalized Audit Software	Snapshot	Tracing	Mapping	Control Flowcharting	Job Accounting Data Analysis	System Development Life Cycle	System Acceptance & Control Group	Code Comparison	Disaster Testing
Operations																	
Transaction Operator					1	2	1	3					3				
Computer Operator	2	2		1		2		3					1			2	1
Peripheral Equipment Operator	2	2		1	1	2	3	3					1				1
Job Set-Up Clerk	2	2				2		3					1			1	
Data Entry & Update Clerk					1	1	1	3									
Communications Operator			3	2	1	1		3					3				1
Media Librarian								3				1	1				1
Software																	
System Programmer	1	1	1	1			1	3	1	1	1	1		1	1	1	
Application Programmer	1	1	1	1			1	3	1	1	1	1	1	1	1	1	
Hardware																	
Terminal Engineer					1	2	2	3	3	3					3	3	1
System Engineer	3	3	3	1		3	3	3	2	3					1	1	1
Communication Engineer	3	3		1	1	3	3	3	1	1					1	1	1
Facilities Engineer																	1
Management																	
Network Manager	3	3		1	1	3	3	3	1	1		2	2				1
Operations Manager	2	2		1	1	2	3	3				2	2				1
Data Base Manager					1	1	1	3	3			3	3				1
Programming Manager	1	1	1	1			1	3	1	1	1	1	1	1	1	1	
Other																	
Identification Clerk					1	1	1	3					3				1
Security Officer																	
EDP Auditor																	

Applicability Codes: 1 – Primary
2 – Secondary
3 – Supportive

Figure 5

Ranking of Tools and Techniques by Number of Occupations Affected –

Tools and Techniques	Number of Occupations Affected
Generalized Audit Software	17
Embeded Audit Data Collection	13
Extended Records	13
Disaster Testing	13
Job Accounting Data Analysis	12
Test Data Method	10
Base Case System Evaluation	10
Parallel Simulation	10
Transaction Selection	10
Code Comparison	9
Snapshot	8
Tracing	7
Control Flowcharting	7
System Acceptance and Control	6
Integrated Test Facility	5
System Development Life Cycle	4
Mapping	3

The following page listing refers the user of this guide to descriptions of each of the 17 audit tools and techniques (including occupations affected by each tool or technique). These descriptions of tools and techniques have been abstracted from *Systems Auditability and Control,* published by the Institute of Internal Auditors, Inc., (International Headquarters, 249 Maitland Avenue, Altamonte Springs, Florida 32701, 1977) and prepared by SRI International in consultation with the IIA. The IIA reports give more detailed descriptions of the 17 tools and techniques.

Page Listing of Audit Tools and Techniques Descriptions

The tools and techniques described in this guide are presented in the same sequence used by the Institute of Internal Auditors, Inc. For the convenience of the user, this page listing is in alphabetical order.

NOTE: Each audit tool or technique described also lists the occupations affected by its use. The user interested in a detailed description of each occupation should refer to Section VIII, Occupation Vulnerabilities.

TEST DATA METHOD

The test data method verifies processing accuracy of computer application systems by executing these systems using specially prepared sets of input data that produce preestablished results. The method gives internal auditors a procedure for the verification of computer programs and applications. It is a method that can be used by internal auditors with only a modest data processing background when testing specific and limited program functions. It is a good technique to use initially in program verification because tests can be expanded incrementally, providing a learning situation for less experienced internal auditors. Special procedures are not usually required. The test data method is limited to computer processing verification and evaluation and is not an appropriate technique for verification of production data. No evidence is provided concerning the completeness or accuracy of production input data or masterfiles.

Occupations Affected:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Job setup clerk	Network manager
Systems programmer	Operations manager
Application programmer	Programming manager

BASE CASE SYSTEM EVALUATION

Base case system evaluation (BCSE) is a technique that applies a standardized body of data (input, parameters, and output) to the testing of a computer application system. This body of data, the base case, is established by user personnel, with internal audit concurrence, as the criterion for correct functioning of the computer application system. This testing process is most widely used as a technique for validation of production computer application systems. One major manufacturing company, however, utilizes the base case approach as a "means to test programs during their development, to demonstrate the successful operation of the system prior to its installation, and to verify its continuing accurate operation during its life." As such, this approach represents a total commitment by corporate management and each user department to the principles and disciplines of BCSE.

Occupations Affected:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Job setup clerk	Network manager
Systems programmer	Operations manager
Application programmer	Programming manager

INTEGRATED TEST FACILITY

Integrated test facility (ITF) is a technique to review those functions of an automated application that are internal to the computer. Internal auditor's test data are used to compare ITF processing results to precalculated test results. The method is most frequently used to test and verify large computer application systems when it is not practical to separately cycle test data. The ITF technique is used for computer processing verification and evaluation and is of limited value for the verification of production data or data files. Limited evidence is provided concerning the completeness and accuracy of production input data or masterfiles.

Occupations Affected:

Communications operator	Systems engineer
Systems programmer	Programming manager
Application programmer	

PARALLEL SIMULATION

Parallel simulation is the use of one or more special computer programs to process "live" data files and simulate normal computer application processing. As opposed to the test data method and the integrated test facility, which process test data through "live" programs, the parallel simulation method processes "live" data through test programs. Parallel simulation programs include only the application logic, calculations, and controls that are relevant to specific audit objectives. As a result, simulation programs are usually much less complex than their application program counterparts. Large segments of major applications that consist of several computer programs can often be simulated for audit purposes with a single parallel simulation program. Parallel simulation permits the internal auditor to independently verify complex and critical application system procedures.

Occupations Affected:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Communications operator	Network manager
Systems programmer	Operations manager
Application programmer	Programming manager

TRANSACTION SELECTION

The transaction selection audit technique uses an independent computer program to monitor and select transactions for internal audit review. The method enables the internal auditor to examine and analyze transaction volumes and error rates, and to statistically sample specified transactions. Transaction selection audit software is totally independent of the production computer application system and is generally parameter-controlled. No alteration to the production computer application system is required. This technique is especially suitable for noncontinuous monitoring and sampling of transactions in complex computer application systems.

Occupations Affected:

- Transaction operator
- Peripheral operator
- Data entry & update clerk
- Communications operator
- Terminal engineer
- Communication engineer
- Network manager
- Operations manager
- Data base manager
- Identification control clerk

EMBEDDED AUDIT DATA COLLECTION

Embedded audit data collection uses one or more specially programmed data collection modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the computer application system at points determined to be appropriate by the internal auditor. The internal auditor also determines the criteria for selection and recording. After collection, other automated or manual methods may be used to analyze the collected data.

As distinct from other audit methods, this technique uses "in-line" code (i.e., the computer application program performs the audit data collection function at the same time it processes data for normal production purposes). This has two important consequences for the auditor: in-line code ensures the availability of a comprehensive or a very specialized sample of data (strategically placed modules have access to every data element being processed); retrofitting this technique to an existing system is more costly than implementing the audit programming during system development. Because of this, it is preferable for the internal auditor to specify his requirements while the system is being designed.

Occupations Affected:

- Transaction operator
- Computer operator
- Peripheral operator
- Job setup clerk
- Data entry & update clerk
- Communications operator
- Terminal engineer
- System engineer
- Communications engineer
- Network manager
- Operations manager
- Data base manager
- Identification control clerk

EXTENDED RECORDS

The extended records technique gathers together by means of a special program or programs all the significant data that have affected the processing of an individual transaction. This includes the accumulation into a single record of results of processing over the time period that the transaction required to complete processing. The extended record includes data from all the computer application systems that contributed to the processing of a transaction. Such extended records are compiled into files that provide a conveniently accessible source for transaction data.

With this technique, the auditor no longer need review several files to determine how a specific transaction was processed. With extended records, data are consolidated from different accounting periods and different computer application systems so that a complete transaction audit trail is physically included in one computer record. This facilitates tests of compliance to organization policies and procedures.

Occupations Affected:

- Transaction operator
- Peripheral operator
- Data entry & update clerk
- System programmer
- Application programmer
- Terminal engineer
- Systems engineer
- Communication engineer
- Network manager
- Operations manager
- Data base manager
- Programming manager
- Identification control clerk

GENERALIZED AUDIT SOFTWARE

Generalized audit software is the most widely used technique for auditing computer application systems. This technique permits the internal auditor to independently analyze a computer application system file. Most generalized audit software packages, because of their widespread use and long history, are ultra-reliable, highly flexible, and extensively and accurately documented. Generalized audit software programs are currently available that can foot, cross-foot, balance, stratify, select a statistical sample, select transactions, total, compare, and perform calculations on diverse data elements contained within various data files. These extensive abilities are available to the internal auditor to substantively test computer application systems. Generally, this audit method is used to test computer file data; little facility is present to test system logic, other than implicitly by the results that appear in the data files. No explicit compliance testing facility is contained in these programs. Historically, generalized audit software programs operated only in the batch mode. Recently, with the rapid expansion of on-line computer application systems, on-line generalized audit software has become available.

Occupations Affected:

- Transaction operator
- Computer operator
- Peripheral operator
- Job setup clerk
- Data entry & update clerk
- Communications operator
- Media librarian
- Systems programmer
- Application programmer
- Terminal engineer
- System engineer
- Communication engineer
- Network manager
- Operations manager
- Data base manager
- Programming manager
- Identification control clerk

SNAPSHOT

Both internal auditors and data processing personnel periodically encounter difficulty in reconstructing the computer decision-making process. The cause is a failure to keep together all the data elements involved in that process. Snapshot is a technique that, in effect, takes a picture of the parts of computer memory that contain the data elements involved in a computerized decision-making process at the time the decision is made. The results of the snapshot are printed in report format for reconstructing the decision-making process.

The snapshot audit technique offers the capability of listing all the data that were involved in a specific decision-making process. The technique requires the logic to be preprogrammed in the system. A mechanism, usually a special code in the transaction record, is added for triggering the printing of the data in question for analysis.

The snapshot audit technique helps internal auditors answer questions as to why computer application systems produce questionable results. It provides information to explain why a particular decision was developed by the computer. Snapshot used in conjunction with other audit techniques (e.g., integrated test facility or tracing) provides the determination of what results would occur if a certain type of input entered the data processing system. The snapshot audit technique also can be an invaluable aid to systems and programming personnel in debugging the application system because it can provide snapshots of computer memory as a debugging aid.

Occupations Affected:

System programmer	Communication engineer
Application programmer	Network manager
Terminal engineer	Data base manager
Systems engineer	Programming manager

TRACING

A traditional audit technique in a manual environment is to follow the path of a transaction during processing. For example, an auditor picks up an order as it is received into an organization and follows the flow from work station to work station. The internal auditor asks the clerk involved what actions were taken at that particular step in the processing cycle. Understanding the policies and procedures of the organization, the internal auditor can judge whether they are being adequately followed.

By the time the internal auditor has walked through the processing cycle, he or she has a good appreciation of how work flows through the organization. In a data processing environment, it is not possible to follow the part of a transaction through its processing cycle solely by following the paperwork flow. Many of the functions performed by clerks and the movement of hardcopy documents are replaced by electronic processing of data.

Tracing is an audit technique that provides the internal auditor with the ability to perform an electronic walk-through of a data processing application system. The audit objective of tracing is to verify compliance with policies and procedures by substantiating, through examination of the path through a program that a transaction followed, how that transaction was processed. It can be used to verify omissions. Tracing shows what instructions have been executed in a computer program and in which sequence they have been executed. Since the instructions in a computer program represent the steps in processing, the processes that have been executed can be determined from the results of the tracing audit technique. Once an internal auditor knows what instructions in a program have been executed, an analysis can be performed to determine if the processing conformed to organization procedures.

Occupations Affected:

Systems programmer	Communication engineer
Application programmer	Network manager
Terminal engineer	Programming manager
Systems engineer	

MAPPING

Mapping is a technique to assess the extent of system testing and to identify specific program logic that has not been tested. Mapping is performed by a software measurement tool that analyzes a computer program during execution to indicate whether program statements have been executed. The software measurement tool can also determine the amount of CPU time consumed by each program segment.

The original intent of the mapping concept was to help computer programmers ensure the quality of their programs. However, auditors can use these same software measurement tools to look for unexecuted code. This analysis can provide the auditor with insight into the efficiency of program operation and can reveal unauthorized program segments included for execution for unauthorized purposes.

Occupations Affected:

System programmer
Application programmer
Programming manager

CONTROL FLOWCHARTING

In a complex business environment, it is difficult to thoroughly understand the total system of control of an organization within its total business and operational context. A graphic technique, or flowchart, for simplifying the identification and interrelationships of controls can be a great help in evaluating the adequacy of those controls and in assessing the impact of system changes on the overall control profile. Flowcharts facilitate the explanation of controls to a system analyst or external auditor, or to personnel unfamiliar with specific operational systems; they also aid in ascertaining that controls are operating as originally intended.

The audit area control flowchart technique provides the documentation necessary to explain the system of control. Often an organization's information about controls is fragmented. This makes it difficult to obtain a clear picture of the controls operating within the organization. The availability of an overall picture of controls, using several levels of flowcharts, facilitates understanding.

Operations Affected:

Communications operator
System programmer
Application programmer
Network manager
Operations manager
Data base manager
Programming manager

JOB ACCOUNTING DATA ANALYSIS

Job accounting facilities are available through most computer vendors as an adjunct to their operating systems. The job accounting facility is a feature of the computer operating system software that provides the means for gathering and recording information to be used for billing customers or evaluating systems usage. Examples of information collected by a job accounting facility are job start and completion times, usage of data sets, and usage of hardware facilities. These job accounting systems were designed by the vendors to serve the operating needs of the data processing department. However, much of the information provided by these facilities is of interest to internal auditors.

Two types of job accounting data, the accounting records and the data set activity records, are of interest to the internal auditor. Accounting records consist of records that show which user used which programs, how often, and for how long. They include an indentification of the user, the hardware features required by the job, the time it took to perform the job, and how the job was completed. Data set activity records provide information about which data files were used during processing and who requested the use of the data sets. Among the information contained in these records are the data set name, record length, serial number of the volumes, and the user of the data set.

The internal auditor can use data from the accounting records to verify charges for use of the computer resources. They also enable the auditor to verify that only authorized individuals use the computer. Data set activity records provide the auditor with a means to verify that data are being used by authorized individuals.

Occupations Affected:

Transaction operator	Application programmer
Computer operator	Network manager
Peripheral operator	Operations manager
Job setup clerk	Data base manager
Communications operator	Programming manager
Media librarian	Identification control clerk

SYSTEM DEVELOPMENT LIFE CYCLE

In computer application programs, careful development can prevent expensive after-the-fact changes. Data processing professionals are increasingly devoting time to reviewing and checking computer application systems during development to minimize costly modifications after installation. EDP auditors are taking advantage of this approach on the part of data processing to strengthen their own review of the development process. In so doing, the auditor and the data processor are ensured that their computer application system objectives are fully met.

Occupations Affected:

System programmer	Operations manager
Application programmer	Programming manager

SYSTEM ACCEPTANCE AND CONTROL GROUP

When the EDP auditor decides to monitor and review the computer application development process, the auditor must determine how to best perform the review. Although the substance of the review is unchanged, the EDP auditor may choose to perform the review personally or to rely on the efforts of another group. To perform the review personally is the choice made by many EDP auditors, even though substantial effort and training may be required to do an effective job. The fact that much of the training required has to do with data processing rather than with EDP auditing has, among other factors, caused the auditors at a large insurance company to choose another approach. The company has established, in the data processing department, a Systems Acceptance and Control (SAC) Group to perform systematic reviews of computer application system developments and to create and maintain effective computer application system standards, particularly in the area of auditability.

Occupations Affected:

System programmer	System engineer
Application programmer	Communication engineer
Terminal engineer	Programming manager

CODE COMPARISON

Code comparison entails comparison of two copies, made at different times, of the program coding for a particular application. The objective of this technique is to verify that program change and maintenance procedures and program library procedures are being followed correctly. The auditor uses the output of the comparison to identify changes that have occurred between the making of the two copies. The auditor then locates and analyzes the documentation that was prepared to authorize and execute the changes. This technique supports compliance testing rather than substantive testing. Code comparison is especially useful for auditing programs that perform critical business functions and are subject to continuing change.

Occupations Affected:

Computer operator	System engineer
Job setup clerk	Communication engineer
System programmer	Operations manager
Application programmer	Programming manager
Terminal engineer	

DISASTER TESTING

Most computer service centers develop plans for dealing with disaster. The disaster testing technique tests the validity of these plans by exercising the methods that would be used in such an event. The disasters provided for may include complete destruction of the computer service center.

The objective of a disaster plan is to ensure effective protection against loss of corporate information. The auditor, on an unannounced basis, simulates a disaster in the computer service center to test the adequacy of the center's contingency plans. The test is performed periodically.

Occupations Affected:

Transaction operator	Communication engineer
Computer operator	Facilities engineer
Peripheral operator	Network manager
Communications operator	Operations manager
Media librarian	Data base manager
Terminal engineer	Identification control
System engineer	clerk

VII EDP CONTROLS

Introduction

Occupations as sources of vulnerabilities are affected by EDP controls in two ways. An individual in an occupation can be the *object of* a control which is meant to constrain that individual's activities. Second, an individual in an occupation can be *responsible for* the operation, implementation, effectiveness or audit of a control. The occupations and corresponding applicable control types are illustrated in the following table, EDP Controls by Occupation Applicability (Figure 6).

Each numbered entry in Figure 6 indicates how applicable a particular control is to the individual who is the object of that control. There are no corresponding degrees of applicability for individuals in occupations responsible (R) for controls.

The following three lists rank the twenty occupations described in this guide by control applicability:

Ranking of Occupations by Number of Applicable Controls —

Object of Controls

Number of Controls Applicable	Occupations
0	Facilities engineer, security officer, EDP auditor
1	Application programmer, systems engineer, programming manager
2	Systems programmer
3	Media librarian
4	Transaction operator, computer operator, data entry and update clerk, network manager, operations manager
5	Peripheral operator, job setup clerk, terminal engineer, communication engineer, data base manager, identification control clerk
6	Communications operator

Responsibility for Controls

Number of Controls Applicable	Occupations
8	EDP auditor, security officer
7	Programming manager
6	Application programmer
4	Systems programmer
3	Systems engineer
1	Communication engineer, facilities engineer, network manager, operations manager
0	All others

EDP CONTROLS BY OCCUPATION APPLICABILITY

Occupations	EDP Controls for Detection & Prevention							
	Transaction Origination	Transactions Entry	Data Communication	Computer Processing	Data Storage and Retrieval	Output Processing	Computer Center	Application System Development
Operations								
Transaction Operator	2	1		1		3		
Computer Operator				1	1	1	1	
Peripheral Equipment Operator		3		1	1	1	1	
Job Set-Up Clerk		3		1	1	3	1	
Data Entry & Update Clerk		1		1	2		1	
Communications Operator	1	2	1	2	3	2	1	
Media Librarian					1	3	1	
Software								
System Programmer			R	R	R	R	1	3
Application Programmer	R	R	R	R	R	R		1
Hardware								
Terminal Engineer	1	R	1	2	2	1		
System Engineer				R	R	R	1	
Communication Engineer	3	3	R	1		1	1	
Facilities Engineer							R	
Management								
Network Manager	3	1	R	1			2	
Operations Manager			3	1	1	1	R	
Data Base Manager		1		1	1/R	2	1	
Programming Manager	R	R	R	R	R	R	1	R
Other								
Identification Clerk	1			1	3	3	1	
Security Officer	R	R	R	R	R	R	R	R
EDP Auditor	R	R	R	R	R	R	R	R

Applicability Codes: 1 – Primary
2 – Secondary
3 – Supportive
R – Responsible for operation or implementation

Figure 6

Ranking of Controls by Number of Occupations Affected —

Controls	Number of Occupations Affected
Computer Center	13
Computer Processing	12
Output Processing	11
Data Storage and Retrieval	10
Transactions Entry	8
Transactions Origination	6
Data Communication	3
Application System Development	2

The following page listing refers the user of this guide to descriptions of the eight primary types of EDP controls. Each description also includes a list of specific controls which are examples of that type, a list of occupations which are the object of that type, and a list of occupations which are responsible for that type of control. These descriptions of control types have been abstracted from *Systems Auditability and Control,* published by the Institute of Internal Auditors, Inc. (International Headquarters, 249 Maitland Avenue, Altamonte Springs, Florida 32701, 1977) and prepared by SRI International in consultation with the IIA. The IIA reports give more detailed descriptions of the eight types of controls.

Page Listing of EDP Controls Descriptions

The types of EDP controls described in this guide are presented in the same sequence used by the Institute of Internal Auditors, Inc. For the convenience of the user, this page listing is in alphabetical order.

NOTE: Each control type described also lists occupations which are the object of or responsible for that control. The user interested in a detailed description of each occupation should refer to Section VIII, Occupation Vulnerabilities.

TRANSACTION ORIGINATION

Transaction origination controls are used to ensure the accuracy and completeness of data before they enter the computer application system. The scope of the transaction origination control area includes controls up to the point of converting data to a machine-readable format. Management, systems personnel, and auditors are placing increasing emphasis on transaction origination controls to ensure that the information prepared for entry into the system is valid, reliable, cost-effective, and not subject to compromise.

Examples of Controls

Origination procedures	Approvals
Forms design	Identification
Document storage	Error handling
Dual custody handling	Manual review
Source data retention	Batch and balance
Separation of duties	Tagging
Authorization	Transmittal

Occupations Object of Controls

Transaction operator	Communication engineer
Communications operator	Network manager
Terminal engineer	Identification control clerk

Occupations Responsible for Controls

Application programmer	Security officer
Programming manager	EDP auditor

DATA PROCESSING TRANSACTION ENTRY

Transaction entry controls are used to ensure the accuracy and completeness of data during their entry into the computer application system. The scope of the transaction entry control area includes controls up to the point of data entering the communication link or, in a nondata communication environment, entry into computer application programs for further processing.

Transaction entry controls are a combination of manual and automated control routines. They are of particular importance because they control two important application areas: data conversion and edit and validation. Increasingly, the emphasis is on automating as many control routines as possible to take advantage of computer hardware abilities and to promote consistency in the application of controls.

Examples of Controls

Written procedures	Data validation
Protected locations	Batch proof and balancing
Terminal data entry	Error handling
Transcription verification	

Occupations Object of Controls

Transaction operator	Communications operator
Peripheral operator	Communication engineer
Job setup clerk	Network manager
Data entry and update clerk	Data base manager

Occupations Responsible for Controls

Application programmer	Security officer
Terminal engineer	EDP auditor
Programming manager	

DATA COMMUNICATION

Data communication controls are primarily concerned with ensuring the integrity of data as they pass through communication lines from the message input devices to the message reception devices. These controls are important because most data communication equipment is owned and controlled by organizations other than the sending or receiving organizations. These controls are also important because there is a fast-growing trend by many organizations to use data communication services as an integral part of their computer application systems. Consequently, to ensure the accuracy and completeness of data for the entire application system, internal auditors are expected to understand and review this area.

Examples of Controls

- Input device identification
- Protected locations
- Message identification and logging
- Message transmission
- Message reception validation and accounting
- Error handling

Occupations Object of Controls

- Communications operator
- Terminal engineer
- Operations manager

Occupations Responsible for Controls

- Systems programmer
- Application programmer
- Communication engineer
- Network manager
- Programming manager
- Security officer
- EDP auditor

COMPUTER PROCESSING

Computer processing controls, which are used to ensure accuracy and completeness of data during computer processing, are the controls that govern computer process integrity and computer process error handling. These controls are applied after the entry of data into the computer application system as application programs process the data. File interface and program interfaces are also included.

The scope of computer processing controls discussed here includes application level controls that are built in and around the central processing unit. These controls are built into each individual application program and control application program data input, processing, and output. Because application controls are unique and specific in one application, they may or may not be transferable between applications. During the continuing development of computer processing controls, it is important to ensure that the principles of internal control (e.g., separation of functions) are being carried forward to the functions performed by the computer application system.

Examples of Controls

- Transaction identification
- Computation and logic
- File balancing
- Operation instructions
- Error handling

Occupations Object of Controls

- Transaction operator
- Computer operator
- Peripheral operator
- Job setup clerk
- Data entry and update clerk
- Communications operator
- Terminal engineer
- Communication engineer
- Network manager
- Operations manager
- Data base manager
- Identification control clerk

Occupations Responsible for Controls

- System programmer
- Application programmer
- System engineer
- Programming manager
- Security officer
- EDP auditor

DATA STORAGE AND RETRIEVAL

Data storage and retrieval controls are important to ensure the accuracy and completeness of data during the process of data storage and retrieval.

The scope of computer data storage and retrieval controls includes those controls in effect during file handling and file error handling. These controls govern the file-handling processes that are not directly associated with the computer processing of the application system.

Data storage and retrieval controls are of particular importance because they involve a high degree of human intervention and data handling. For this reason it is important to provide the facility and personnel procedures necessary to control the integrity of data files and programs during intermediate storage and retrieval.

Examples of Controls

- Library procedures
- File access
- File maintenance
- Backup
- Error handling

Occupations Object of Controls

- Computer operator
- Peripheral operator
- Job setup clerk
- Data entry and update clerk
- Communications operator
- Media librarian
- Terminal engineer
- Operations manager
- Data base manager
- Identification control clerk

Occupations Responsible for Controls

- System programmer
- Application programmer
- System engineer
- Programming manager
- Security officer
- EDP auditor

OUTPUT PROCESSING

Output processing controls are used to ensure the integrity of output data from the conclusion of computer processing until their delivery to the functional user.

The functional user is dependent on the prompt delivery of complete and accurate data to conduct the day-to-day business functions. If the organization has proper input and processing controls, computer output is usually correct. However, output controls play an important part in achieving the control objectives associated with the overall computerized record-keeping system. The function of output control is to ensure that processed information includes authorized, complete, and accurate data. The scope of output controls includes the control areas of data processing balancing and reconciliation, output distribution, user balancing and reconciliation, records retention, accountable documents control, and output error handling.

Output controls are important as a control interface between the functional user and data processing. The primary method by which data processing and users ensure that the integrity of data has been maintained during processing is by monitoring application system output.

Output controls are those controls that can be used to control the output and distribution of information from the computer application system.

Examples of Controls

- Reconciliation, logging and review
- Handling and distribution
- User balancing and reconciliation
- Retention and disposal
- Accountable document handling
- Error handling

Occupations Object of Controls

- Transaction operator
- Computer operator
- Peripheral operator
- Job setup clerk
- Communications operator
- Media librarian
- Terminal engineer
- Communications engineer
- Operations manager
- Data base manager
- Identification control clerk

Occupations Responsible for Controls

- Systems programmer
- Application programmer
- System engineer
- Programming manager
- Security officer
- EDP auditor

COMPUTER SERVICE CENTER

The accuracy and completeness of records and reports produced by the data processing function depends on the general controls governing computer service center operations and on application controls. Inadequate controls within the computer service center or failure to comply with established controls can result in errors in data preparation and handling, production scheduling, file updating and output report preparation. The controls are functionally independent of application controls but are of equal importance to the accuracy of the results of data processing. The failure of general controls within the computer service center can defeat the objectives of the most elaborate application controls. As such, controls are of great concern to both data processors and internal auditors. The importance of this is demonstrated by survey results, which state the most important goals or objectives of internal auditing when reviewing the data processing department:

- Development of more built-in audit controls
- Enhancement of security (data access, separation of duties, etc.)
- Monitoring methods and procedures to ensure accurate data processing performance.

Computer service center controls can contribute substantially to the fulfillment of all of these objectives.

Examples of Controls

- Input/output scheduling
- Media library
- Malfunction reporting and repair
- Environment and physical security
- Separation of duties
- Billing and charge-out
- Disaster recovery

Occupations Object of Controls

- Computer operator
- Peripheral operator
- Job setup clerk
- Data entry and update clerk
- Communications operator
- Media librarian
- Systems engineer
- Communications engineer
- Network manager
- Data base manager
- Programming manager
- Identification control clerk

Occupations Responsible for Controls

- Facilities engineer
- Operations manager
- Security officer
- EDP auditor

APPLICATION SYSTEM DEVELOPMENT

The adequacy and effectiveness of controls included in computer application systems are affected by the methods and procedures used during the system development process. Controls over the system development process are important for three reasons:

(1) Good development controls assist in managing costs and schedules.

(2) They help ensure that appropriate application controls are built into application systems being developed.

(3) They ensure that application controls are properly tested before application systems become operational.

By carefully controlling the system development process, one can achieve higher levels of accuracy and reliability in the computer application systems developed and satisfy the goals of developing quality application systems within cost and on schedule.

Elements of the application system development process documented by SRI include project management, programming techniques, development and acceptance testing, program change control, documentation, and data base administration. Each of these elements is discussed in this chapter. Specific techniques and controls within each element identified during the study are presented within the relevant sections of the chapter.

Examples of Controls

- Life cycle step reviews
- Structural program audit trail
- Acceptance testing
- Program change review
- Documentation review
- Data base administration

Occupations Object of Controls

- System programmer
- Application programmer

Occupations Responsible for Controls

- Programming manager
- Security officer
- EDP auditor

VIII OCCUPATION VULNERABILITIES

Introduction

This is the primary section of this guide. It provides a 2-page description and analysis of each of the 20 EDP and EFT occupations in the EDP and data communications environment. Each occupation description includes the following information:

Page One

Job Title – The job titles are based on EDP practices and are variations of job titles in the IBM manual, *Organizing the Data Processing Activity* (Gc20-1622-2). These titles will not conform exactly to positions in EDP and EFT participant organizations, and adaptation for individual organizations is required.

Employers – The most probable employers among EFT participants are identified (e.g., merchant, financial institution, etc.)

Function – A brief description of duties is given. Like the job title, these functions are variations of descriptions in *Organizing the Data Processing Activity.* Adaptation is necessary to match the duties listed with those of a position in a particular organization. It is assumed that the manager of the individuals in each occupation is included in that occupation description and that the manager will have no more skills, knowledge, or access than the employee managed. Exceptions are accommodated by including four management positions among the occupations. These positions are included because they span the skills, knowledge, and access of more than one occupation or occupy particularly sensitive positions in EDP. Also listed under 'Function' are important knowledge, important skills, important access, and the manager to whom the person in the occupation reports. The knowledge and skills usually possessed by a person in the occupation are presented in list form. Also included are the work-related and functional material to which the employee has access.

Conclusions – Additional insights, further descriptions of vulnerabilities, and particular dangers and remedies are included.

Vulnerabilities – The classes of vulnerabilities (physical, transactional, programming, and electronic) are stated for each occupation. Descriptions of these classes are provided in Section V. The most commonly listed items in this column are modification, destruction, disclosure (a broad term which includes talking, taking copies, or revealing in any way), and use (a term which describes accidental or intentional acts). The most likely vulnerabilities are also emphasized in the 'Conclusions' portion of Page One.

Each occupation and its vulnerabilities is presented assuming no collusion with others and no use of the knowledge, skills, or access of other occupations. As such, vulnerabilities are described at the most basic level of unauthorized activities. The combinations of skills, knowledge, and access necessary for collusion is too complex to be detailed in this guide. Nevertheless, the possibilities for collusion should be considered seriously by the user of this guide. Almost half of the reported computer related financial institution fraud and embezzlement has involved collusion – a far higher proportion than similar manual crimes (less than 4% in one set of cases reported by the Comptroller of the Currency). The high frequency of collusion in computer related crime may occur because such crimes often require more skills, knowledge, and access than those possessed by a person in a single EFT occupation. This is supported by examining the limitations of the occupations described in this guide. The greater

vulnerabilities are found in those occupations that span several EFT functions (such as systems programmers and engineers, auditors, and security officers).

Studying the possible individual vulnerabilities demonstrates that an error or omission caused by a single individual's careless or incompetent act results in a minimal loss. It is the frequency of errors and omissions which raises the problem to serious levels. Errors and omissions are usually loss limited (i.e., when repetition occurs, the size of the loss grows to the point at which it becomes visible and is then stopped). Intentional, unauthorized acts are designed by the perpetrator to prevent this from occurring, at least until it is too late for the victim to recover. One exception is the single error that causes massive destruction in a system by fast propagation of loss. This could occur in EFT. Another exception is the error or omission that facilitates an intentional act of serious magnitude.

Controls — The types of controls an individual in the occupation is the *object of* are listed, immediately followed by the types of controls the individual is *responsible for.* Detailed descriptions of the control types are listed in Section VII.

Audit Tools and Techniques — Audit tools and techniques are identified which can be used to detect accidental and intentional acts by a person with the described skills, knowledge, and access. Detailed descriptions of the audit tools and techniques are provided in Section VI.

Page Two

The second page illustrates the vulnerable areas of knowledge, skills, functional access, and physical access for the particular occupation. The same graphic is used for each occupation; only the shaded areas differ to identify vulnerabilities which apply to that occupation. This method is used to enable the guide user to see at a glance which areas represent vulnerabilities which apply to that occupation and which areas do *not.* This is particularly important as the occupations are all based on identified skills, knowledge, and access. Employees must first be identified on the basis of their skills, knowledge, and access authorization. Only then can they be matched with one or more of the 20 occupations described.

The potential for reducing vulnerabilities is greatest for occupations with the least ability to make changes, with the narrowest range of knowledge, and with the most structured working environment. Other occupations possess a wider range of knowledge, skills, and access and there is a lack of applicable audit tools and techniques and controls. These occupations are in the highest position of trust. They possess the greatest potential for performing significant unauthorized acts with little possibility of detection or apprehension. This is illustrated in the following four tables (Figures 7, 8, 9, and 10):

KNOWLEDGE BY EDP AND EFT OCCUPATIONS

Occupations	Knowledge: Data Files: Application Program Library	Accounts/ Master Files	Transactions/ File Update Data	Security Codes	Operating System Programs	Testing Programs/ Data	History Files Off-Line/On-Site	Remote Storage	Documentation: Operating System/ Sysgen	Application Programs/ Data Layout	Data Base Structure	Circuit/ Network Diagrams	Procedural	Hardware: Computer Equipment	Communications Equipment	Programmer Terminals	Remote Terminals	Facilities Equipment/ Power Air	Production Control: Job Set-up	User Output
Operations																				
Transaction Operator			X										X				X			
Computer Operator	X	X	X	X	X	X	X		X				X	X				X		
Peripheral Equipment Operator	X	X	X			X	X						X	X				X	X	X
Job Set-Up Clerk							X				X		X						X	X
Data Entry & Update Clerk		X									X		X				X			
Communications Operator						X						X	X	X	X	X	X			
Media Librarian	X	X			X	X	X	X					X							
Software																				
System Programmer					X	X			X		X		X	X	X	X	X			
Application Programmer						X				X			X			X			X	X
Hardware																				
Terminal Engineer			X			X						X	X		X	X	X			
System Engineer					X	X			X			X	X	X	X	X	X	X		
Communication Engineer												X	X		X					
Facilities Engineer												X	X	X				X		
Management																				
Network Manager									X			X	X	X	X					
Operations Manager					X		X	X	X		X		X	X	X	X		X	X	X
Data Base Manager		X					X				X		X			X				
Programming Manager		X				X				X	X		X			X				
Other																				
Identification Clerk			X				X						X			X			X	X
Security Officer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
EDP Auditor	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Figure 7

SKILLS BY EDP AND EFT OCCUPATIONS

Occupations	Skills: Operations: Terminal/ keyboard	CPU Console	Communication Equipment	EDP Peripheral Equipment	Electronic Test Equipment/Tools	Electronic Fabrication	Plastic Card Embossing/ Encoding Equipment	Record Keeping, Filing	Interpretive/Analytical: Read Memory Dumps	Read Flowcharts/Hipo Diagrams	Read Circuit Schematics	Read Diagnostic/ Error Codes	Convert Binary to Character	Write Logical Expressions	Draw Flowcharts/Diagrams/Circuits	Perform Systems Analysis	Read Procedural Documentation
Operations																	
Transaction Operator	X																X
Computer Operator		X										X					X
Peripheral Equipment Operator				X													X
Job Set-Up Clerk																	X
Data Entry & Update Clerk	X											X					X
Communications Operator			X		X						X	X					X
Media Librarian								X									X
Software																	
System Programmer	X	X	X	X					X	X		X	X	X	X	X	X
Application Programmer	X								X	X		X	X	X	X	X	X
Hardware																	
Terminal Engineer	X		X		X	X				X	X	X	X				X
System Engineer	X	X	X	X	X	X			X		X	X	X	X	X		X
Communication Engineer			X		X	X					X	X					X
Facilities Engineer					X						X						X
Management																	
Network Manager											X	X				X	X
Operations Manager	X	X		X					X			X				X	X
Data Base Manager	X									X						X	X
Programming Manager										X						X	X
Other																	
Identification Clerk	X						X										X
Security Officer	X		X	X	X		X		X	X	X	X				X	X
EDP Auditor	X		X	X			X		X	X	X	X	X	X	X	X	X

Figure 8

PHYSICAL ACCESS BY EDP AND EFT OCCUPATIONS

Occupations	Physical Access Areas												
	Transactional	Data Communications	Computer	Peripheral Equipment	Media Library	Input/Output Handling	Facilities Equipment	Back-up Storage Site	Communications Company	Programming Offices	Audit Office	Security Office	Data Preparation
Operations													
Transaction Operator	X												
Computer Operator			X										
Peripheral Equipment Operator				X									
Job Set-Up Clerk						X							
Data Entry & Update Clerk	X												X
Communications Operator		X							X				
Media Librarian					X			X					
Software													
System Programmer		X	X	X						X			
Application Programmer										X			
Hardware													
Terminal Engineer	X			X					X	X			
System Engineer		X	X	X									X
Communication Engineer		X							X				
Facilities Engineer							X						
Management													
Network Manager		X							X				
Operations Manager		X	X	X	X	X		X					X
Data Base Manager				X		X		X					X
Programming Manager										X			
Other													
Identification Clerk				X		X							X
Security Officer	X	X	X	X	X	X	X	X	X	X	X	X	X
EDP Auditor	X	X	X	X	X	X	X	X	X	X	X	X	X

Figure 9

FUNCTIONAL ACCESS BY EDP AND EFT OCCUPATIONS

Occupations	Functional Access																							
	Software			Hardware			Procedures											Concepts						
	Application Data Base Programs Language	Operating System Communications Utilities	Modeling Simulation	Digital Logic Design	Electronic/ Electro-Mechanical Engineering	Communication Engineering	Programmer Terminals Protocol	Remote Point-of-Transaction Terminals	CPU Console Protocol	Data/ File/ Library/ Job Accounting	System Integration/ Testing/ Interfaces	Physical Access Control	Security Identification	EDP Production Workflow	Authorization Limit Controls	Account Number Standards	Accounting	Data Base/ Data Communications	Computer Architecture	Boolian Logic	Structured Design/ Programming	Inventory Control
Operations																								
Transaction Operator								X					X		X	X								
Computer Operator									X	X		X	X	X				X						
Peripheral Equipment Operator										X		X		X										
Job Set-Up Clerk										X		X		X										
Data Entry & Update Clerk	X						X			X		X	X	X				X						
Communications Operator		X						X				X	X					X						
Media Librarian										X		X		X										X
Software																								
System Programmer		X	X				X		X	X	X	X	X	X				X	X	X	X	X		
Application Programmer	X		X				X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Hardware																								
Terminal Engineer		X		X	X	X	X	X				X	X					X		X				
System Engineer		X		X	X	X	X		X			X	X					X	X	X				
Communication Engineer				X	X	X						X								X				
Facilities Engineer					X							X												
Management																								
Network Manager		X				X					X	X	X					X						
Operations Manager		X					X		X	X	X	X	X	X				X	X					
Data Base Manager	X						X			X	X	X	X	X	X	X		X						
Programming Manager	X									X	X	X	X	X			X		X	X	X	X		
Other																								
Identification Clerk										X			X											
Security Officer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
EDP Auditor	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Figure 10

Page Listing of Occupation Descriptions

The occupations described in this guide are presented in a sequence which corresponds to the life cycle of an EDP system. For the convenience of the user, this page listing is in alphabetical order.

NOTE: The audit tools and techniques named in the occupation descriptions are described in Section VI. The EDP controls listed are described in Section VII.

TRANSACTION OPERATOR

Employers. Merchant, financial institution, hardware/software maintenance vendor.

Function. Transaction operators operate an EFT transaction terminal by entering funds transfer transactions at the direction of customers or the employer.

Important Knowledge:	Terminal protocol Identification verification procedures Authorization limits Account number standards Other procedural controls
Important Skills:	Typing and keyboard functions operation Manual dexterity Basic reading ability
Important Access:	Terminal area Instructional documentation Identification verification materials at the time of use Account files
Reports to:	Sales management

Conclusions. Transaction operators function like a teller for financial institutions. Therefore, traditional teller controls are applicable. There are several vulnerabilities related to inactive and dormant accounts which include deceiving customers, lapping fraud, and kiting. The identification verification function requires complete instructions and careful training. The high degree of transaction automation provides for extensive controls in the system to cause both real time and non-real time exception reporting for any deviations from normal activity. All transactions and functions performed by the operators must be identifiable in computer files as having been performed by them for audit trail purposes.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical & Transactional: Modifying, destroying, or disclosing and using ID verification materials belonging to operator or others Using terminal functions to change account data and balances Physically destroying the terminal	**Object of:** Transactions origination Transactions entry Computer processing transaction identification Output processing reconciliation and review **Responsible for:** None	Selected transaction audit Embedded audit data collection Extended record audit Generalized audit software Terminal access accounting analysis Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

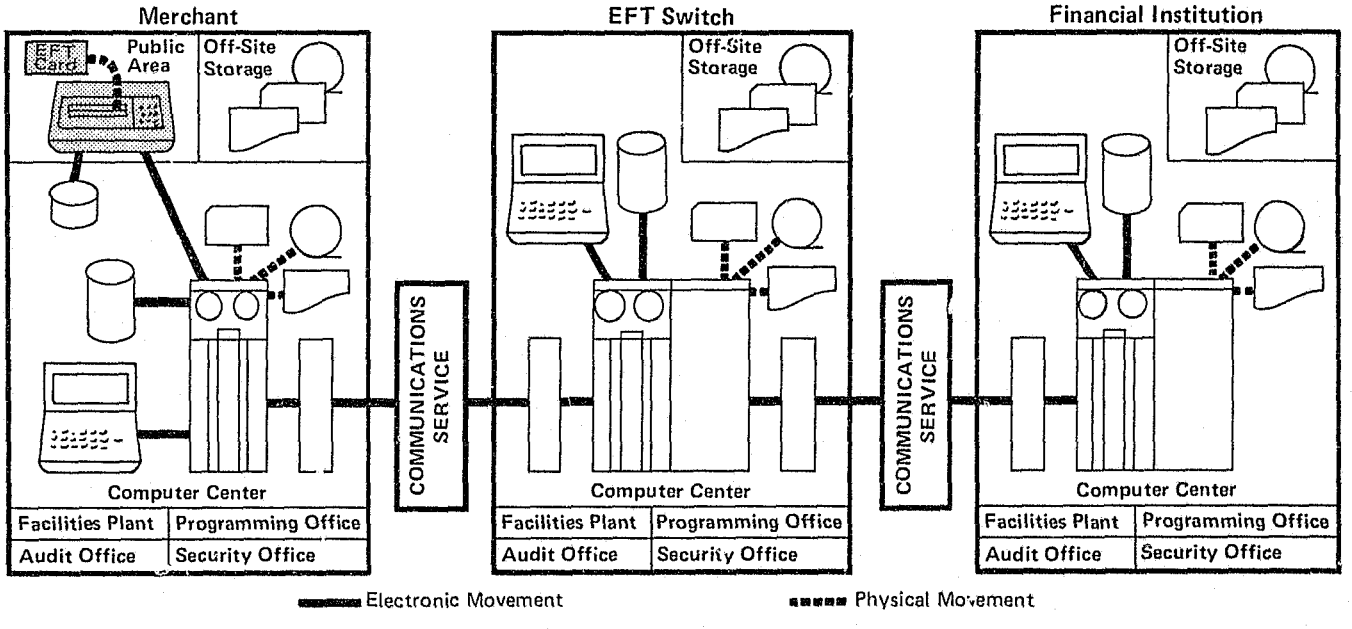
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



COMPUTER OPERATOR

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau.

Function. The computer operator operates the computer from the computer console; alters job schedules and priorities through the console input device; initiates utility program execution; mounts magnetic tapes on magnetic tape drives and disk packs on disk drives; responds to system and application error conditions according to documented operating instructions; and powers up and powers down the computer system.

Important Knowledge:	Operating systems components Utility program functions Console protocol Job names and accounting Privileged access passwords EDP production workflow Data base file names Physical access procedures
Important Skills:	Typing Reading and interpreting console messages Reading procedural documentation Operating computer equipment
Important Access:	Computer equipment room Maintenance area Privileged access to the entire contents of the computer system and externally stored files Procedural documentation
Reports to:	Operations manager

Conclusions. Any action that could be performed in the computer system or in other computer systems in a network through the use of computer utility programs and console commands can be performed by the computer operator. He is limited only to the extent that he cannot alter computer programs or write his own computer programs. He must rely on already available utility programs and console functions. He is also limited by the lack of detailed knowledge of file formats and contents, detailed processing, and control functions. One of the best control functions is to maintain the integrity of the console log printout which records most of the activities of the computer operator and to examine the log in detail. Application systems should minimize the need for computer operator activity and knowledge of application functions. The auditor's reliance on computer operation services is one of the most significant factors in reducing the auditor's independence. Auditing should be performed with as little involvement of computer operators as possible. Controls on the use of utility programs for only intended purposes is another important security function. All audit tools and techniques involving the computer should be used on a separate computer or at least independent of the operator being audited.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical & Transactional: Modification, disclosure, or destruction of the contents of the computer system, externally maintained files, or data files stored in other electronically connected computer systems Use of the computer system for unauthorized purposes Physical destruction of the computer and related facilities	**Object of:** Computer processing Data storage and retrieval Output processing Computer Center **Responsible for:** None	Test data method Base case system evaluation Parallel simulation Transaction selection Embedded audit data collection Generalized audit software Job accounting data analysis Code comparisons Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

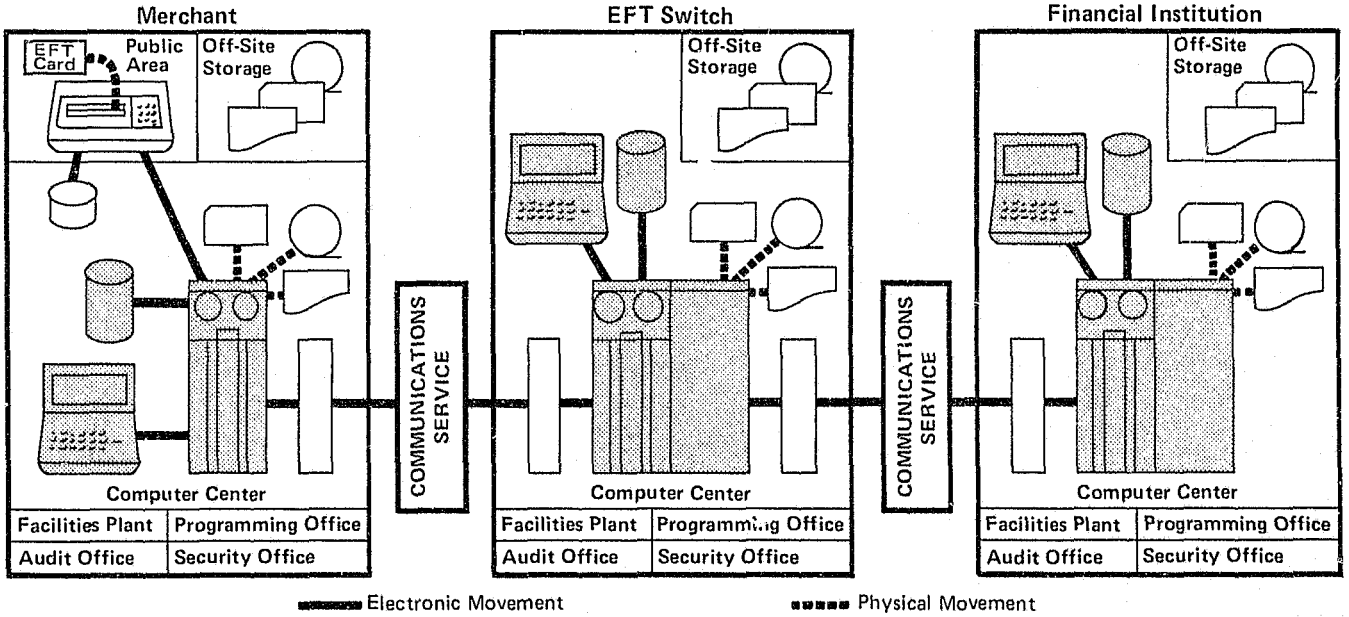
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



PERIPHERAL EQUIPMENT OPERATOR

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau.

Function. Peripheral equipment operators operate all equipment immediately peripheral to the computer and related to input/output and data file use. They operate card readers, printers, optical reading devices, sorters, tape drives, disk drives, tape cleaners, card punches, optical readers; make data files available to the computer system; add data to an input stream; remove disks, punch cards, and printed output; provide expendable supplies for peripheral equipment, e.g., continuous forms, punch cards, and printer ribbons.

Important Knowledge:	Data files Media library Job accounting Expendable supplies Physical access procedures EDP production workflow
Important Skills:	Peripheral equipment operation Microfilm/Microfiche equipment operation Reading procedural documentation
Important Access:	Peripheral equipment Production and job set-up areas User output distribution areas Input data and output data
Reports to:	Operations manager

Conclusions. The greatest concerns about peripheral equipment operators include: handling and misusing negotiable instruments; copying or taking data files and computer programs; and physically destroying data, programs, equipment, and facilities. The advancement of EFT applications will considerably reduce exposure to input, negotiable instrument manipulation, and output. Increasing use of on-line program libraries will reduce exposure to computer programs under development and in production. Job functions overlap with computer operators and transaction operators. The best controls are manual and automated accounting for supplies (especially negotiable instrument forms), automated controls on input and output, and confirmation of input transactions and output distribution.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical & Transactional: Modification, disclosure, or destruction of input data, output data, media, and expendable supplies, including negotiable instrument forms, negotiable instruments, and canceled negotiable instruments Physical destruction or removal of peripheral equipment Modification of job scheduling	**Object of:** Transaction entry Computer processing Data storage and retrieval Output processing Computer center **Responsible for:** None	Test data method Base case system evaluation Parallel simulation Transaction selection Embedded audit data collection Extended records Generalized audit software Job accounting data analysis Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

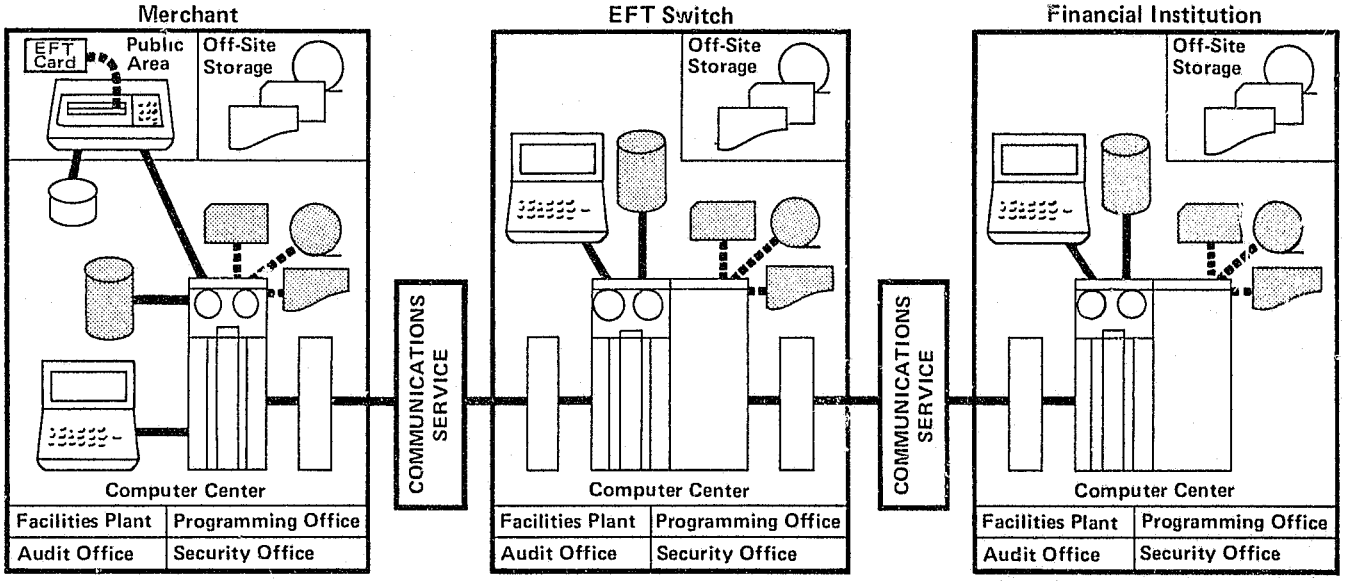
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



JOB SET-UP CLERK

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau.

Function. Job set-up clerks assemble jobs which includes data, computer programs, and job control information. They request that jobs be executed, request media libraries for data, physically place jobs and data into production job queues, and handle procedures for reruns and user requests. They may also distribute output from the jobs to the users.

Important Knowledge:	Data files Media library contents Job accounting procedures Physical access procedures Production workflow
Important Skills:	Reading ability for documentation Manual dexterity for handling tapes and punching cards
Important Access:	Procedural and data base documentation Limited off-line files and some media storage Job set-up and user output areas
Reports to:	Operations manager

Conclusions. This individual does not generally know the content of data files and knows only a small amount about the computer program functions. The threat of fraud is minimal. Since copying facilities are not available, there is also minimal danger that copies of data or programs will be taken. Destruction of data and programs for the purpose of vandalism is more likely. Unauthorized use of computer services is possible by initiating unauthorized jobs, but the jobs would be limited to the computer programs available to the job set-up clerk. The best control is confirmation of job initiation and output delivery among computer services users. This individual is in one of the positions of least trust.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical & Transactional: Modification, disclosure or destruction of data files, computer programs, or data media Unauthorized use of computer services Misuse of output	**Object of:** Transactions entry Computer processing Data storage and retrieval Output processing Computer center **Responsible for:** None	Test data method Base case system evaluation Embedded audit data collection Job accounting data analysis Code comparison

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

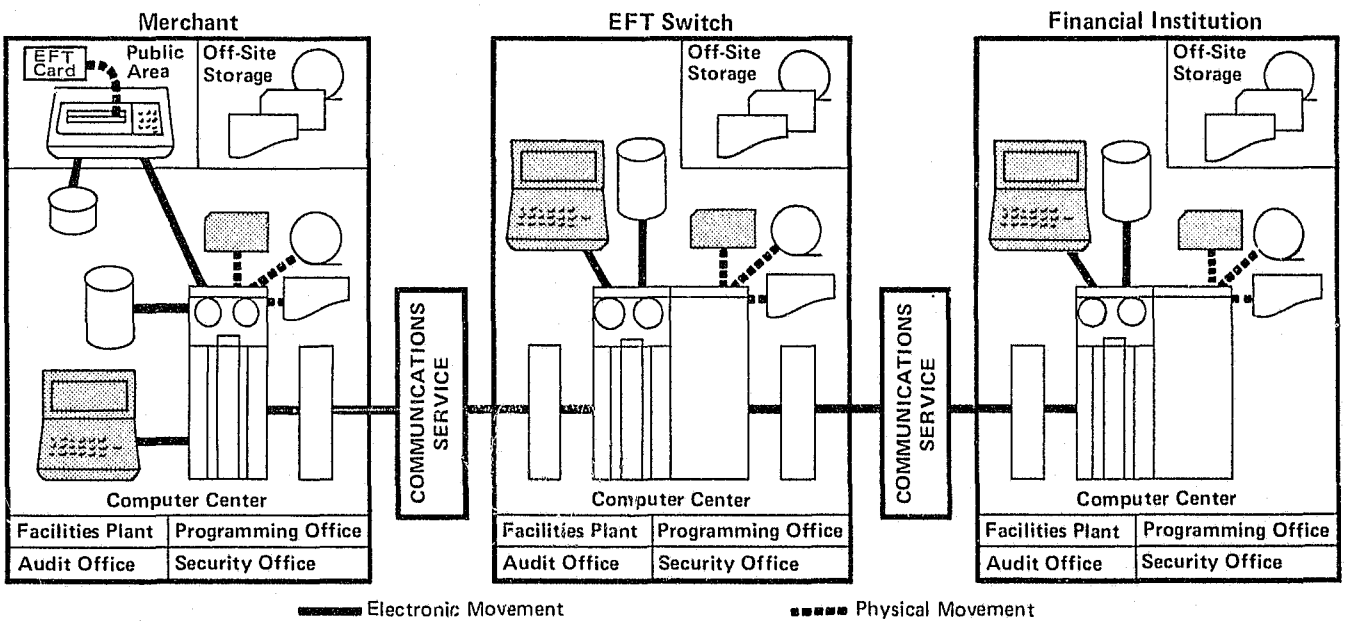
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



DATA ENTRY AND UPDATE CLERK

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau.

Function. Data entry and update clerks add, change, or delete records from on-line data bases by means of an on-line terminal. They also manually update card decks or entries on input data forms.

Important Knowledge:	Data base languages Terminal protocol Data base records, files, formats, and content Security access controls Some job production workload procedures Data base concepts
Important Skills:	Typing Reading procedural documentation
Important Access:	On-line files Documentation on data base structure and content Procedural documentation On-line terminal
Reports to:	Data base manager

Conclusions. Data entry and update clerks are in a position of great trust because they are responsible for handling exception situations, data entry, and transaction errors. The best protection is through dual control over changes, separation of responsibility for authorization of changes, analysis of the data base change log, and customer confirmations. Data base language facilities should be available to only those individuals necessary for carrying out the function.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical & Transactional: Modification, destruction, or disclosure of data base contents, such as customer account files Physical damage to the on-line terminal	**Object of:** Transaction entry Computer processing Data storage and retrieval Computer center **Responsible for:** None	Transaction selection Embedded audit data collection Extended records Generalized audit software

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

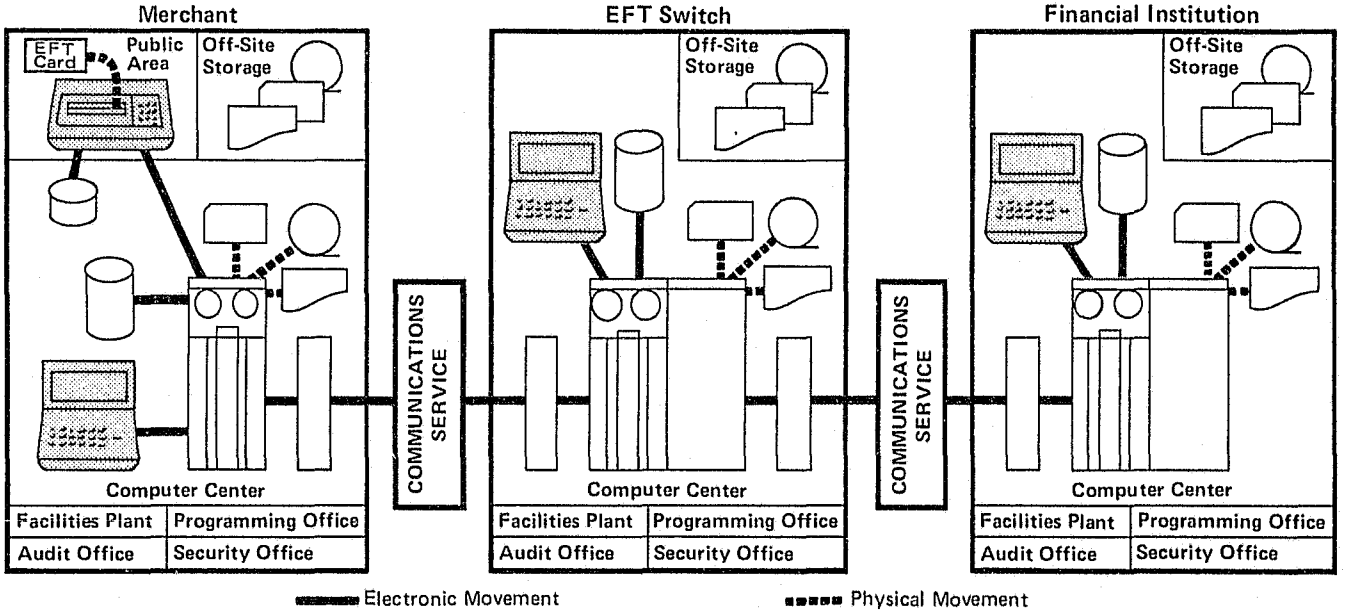
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



COMMUNICATIONS OPERATOR

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau, telephone company, maintenance and equipment vendors.

Function. Communications operators operate communication equipment necessary for an EFT network, including concentrators, multiplexors, modems, and line switching units. They also reconfigure the network when there are failures or overload situations.

Important Knowledge:	Communication theory Function of communication equipment and communication equipment Diagnostic and error codes Point of transaction and programming terminals protocol Physical access and security identification procedures
Important Skills:	Communication and electronic test equipment operation Reading circuits schematics and procedural documentation Typing and keyboard function operation
Important Access:	Communication and terminal equipment and adjacent areas Procedural documentation
Reports to:	Operations manager

Conclusions. Lack of application knowledge concerning EFT functions effectively limits these individuals from fraudulent activities. Errors, omissions, and vandalism are much more likely. Also, the operators are in a position to cause the disclosure or false entry of large amounts of data. However, they would be unlikely to know very much about the purpose or effect of such activities.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, & Electronic: Modification, destruction, or disclosure of communicated data using terminal functions, electronic equipment modification, or communications software modification to change or redirect account data and balances Destruction of data equipment or facilities Use of communication services for unauthorized purposes, including vandalism, through overloading or misdirecting data communication channels	**Object of:** Transaction origination Transaction entry Data communication Computer processing Data storage and retrieval Output processing Computer center **Responsible for:** None	Integrated test facility Parallel simulation Transaction selection Embedded audit data collection Generalized audit software Control flowcharting Job accounting data analysis Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

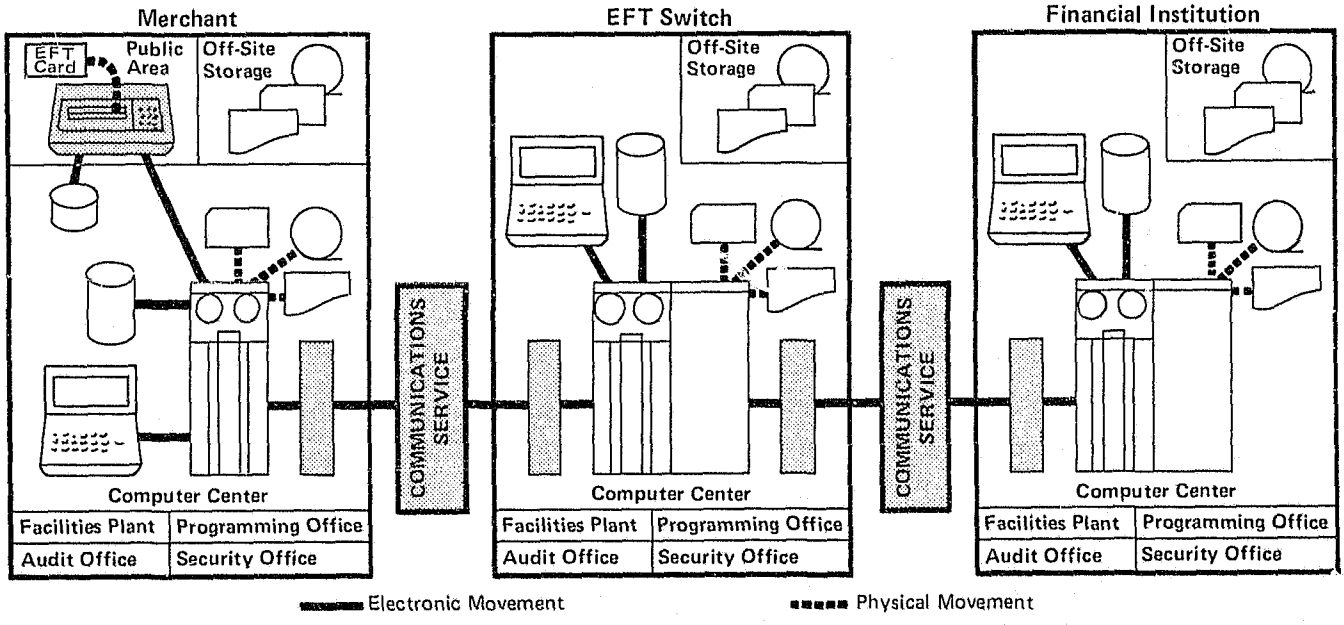
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



MEDIA LIBRARIAN

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau.

Function. Media librarians file, retrieve, and account for off-line storage of data on disk, tape, cards, or other removable media. They also provide media for the production control and job set-up areas and functions, and cycle back-up files through the remote storage facilities.

Important Knowledge:	Data file names and labels Library and job accounting procedures Physical access procedures Production workflow Archived data files
Important Skills:	Reading procedural documentation and computer listings Record keeping Filing Inventory control
Important Access:	Current and previous generations of program libraries All data files, including test programs and data Interface to off-site remote storage facilities and production control Media library facilities
Reports to:	Operations manager

Conclusions. Lack of knowledge of the contents and functions of files and computer programs limits the likelihood of fraud for this position. Errors or the intent to vandalize are more serious. The most effective controls are internal label checking of all media mounted on-line and standard inventory control auditing procedures. The location of the media library and limited access control are also of great importance. Restriction of media movement to computer and peripheral areas, media library, and remote backup storage facilities significantly reduces exposure to data media losses.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical: Destruction and disclosure of computer programs and data files Destruction or taking of media Substitution of incorrect programs or data files for computer processing	**Object of:** Data storage and retrieval Output processing Computer center **Responsible for:** None	Generalized audit software Job accounting data analysis Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

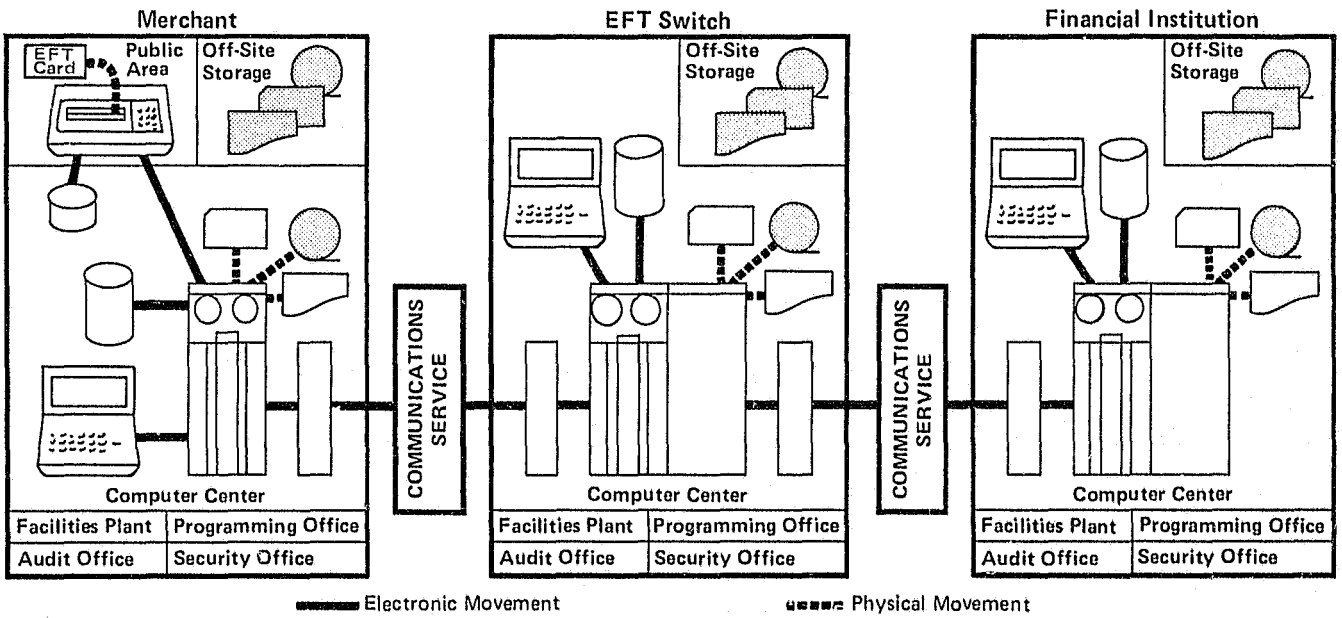
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



SYSTEMS PROGRAMMER

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau, computer and maintenance vendors, software vendor.

Function. Systems programmers design, develop, install, modify, document, and maintain operating system and utility software. Operating system software includes: programming language compilers, loaders, linkage editors, input/output routines, storage managers, program library access and maintenance routines, terminal and communication line handlers, system debugging and testing facilities, system access controls, job schedulers, system accounting routines, and interrupt and trap servicing programs.

Important Knowledge:	Computer operating systems Programming languages Terminal and computer console protocols Security identification Job production workflow Computer architecture Boolean logic Physical access Number systems and alphanumeric codes
Important Skills.	Programming and documentation Computer and peripheral equipment operation Reading and analyzing computer storage dumps and flowcharts Diagnostic analysis
Important Access:	Programming offices System documentation Computer and peripheral equipment facilities Computer system and data communication system (privileged access)
Reports to:	Operations or programming manager

Conclusions. Systems programmers are in the position of greatest trust. They are limited in their actions primarily by physical access control, dual control over their programming work, independent system and control group functions, and their lack of knowledge of applications. Few audit tools and techniques are able to detect intentional acts because systems programmers can easily overcome them. Some audit tools and techniques apply to errors and omissions, but few auditors possess the technical ability to sufficiently understand computer operating systems. Computer system controls are of little value since systems programmers are responsible for their design, implementation, and maintenance. The systems programmers who are employees of the computer and peripheral equipment vendors must also be considered potential vulnerabilities because making covert modifications and introducing trap doors and logic bombs are possible through Trojan horse techniques.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, & Programming: Modification, disclosure, or destruction of any contents of the computer and data communications system in a network, including all computers and terminals, either through direct real time actions or in non-real time actions through modification and use of operating systems or utility programs Physical destruction or modification of computer and peripheral equipment	**Object of:** Computer center Application system development **Responsible for:** Data communication Computer processing Data storage and retrieval Output processing	Test data method Base case system evaluation Integrated test facility Parallel simulation Extended records Generalized audit software Snapshot Tracing Mapping Control flowcharting System development life cycle System acceptance & control group Code comparison

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

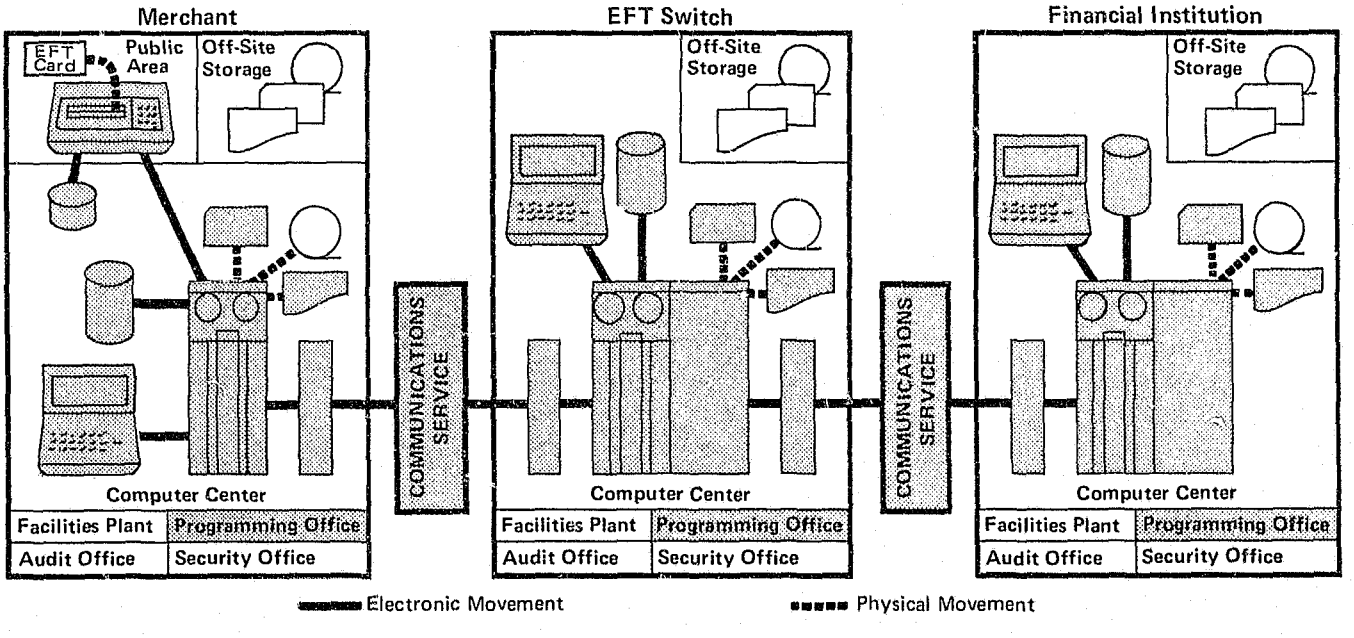
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



APPLICATION PROGRAMMER

Employers. Merchant, financial institution, EFT switch, facilities management contractor, service bureau, computer and software vendor.

Function. Application programmers design, develop, debug, install, maintain, and document computer application programs and systems using a variety of assembly and compiler languages.

Important Knowledge:	Application program languages EDP procedures and concepts EFT applications
Important Skills:	Programmer terminal operations Reading computer programs, memory dumps, flowcharts and diagnostics Writing logical expressions Drawing flowcharts Performing systems analysis
Important Access:	Application programming offices Test programs Test data Application programs Data file documentation Procedural documentation Programmer terminal Computer production control area
Reports to:	Programming manager

Conclusions. Application programmers represent as significant a vulnerability as the systems programmers. Vulnerabilities from application programmers are generally localized to familiar application programs. Usually they can make unauthorized changes to these application programs with very little chance that they will be detected. They are also the last to handle a program before production use in a sequence of personnel who have specified and implemented the requirements for the application. Errors, omissions, and intentional acts made by them tend to be the most dangerous and can result in large losses. Programmers sometimes assume that they have ownership rights to software that they developed for their employer. Programmers will sometimes exchange programs with other programmers or give copies of programs to unauthorized people on an informal basis. The best controls for this occupation are random reviewing of application programs by EDP auditors; limiting programmers in detailed knowledge of application programs and parts of application programs not essential to their work; and independent software testing and assurance results in reviews of all application programs and program changes for integrity and correctness. Formal procedures should be established to assign staff, develop, check out, and prepare for production status with formal transition procedures between each step. Programmers should have limited and controlled access to all production program listings. Copies of listings should be logged in and out of a centralized programming library.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, & Programming: Modification, disclosure, or destruction of data files and computer programs through modifications of application programs during development, debugging, and maintenance. Usually, this would occur only with programs familiar to the programmer. Application programs may be copied and taken when they have trade secret value. Unauthorized use of computer services Vandalism to application programs and data files and denying use of computer programs can be done for extortion purposes.	**Object of:** Application system developement **Responsible for:** Transactions origination Transactions entry Data communication Computer processing Data storage and retrieval Output processing	Test data method Base case system evaluation Integrated test facility Parallel simulation Extended records Generalized audit software Snapshot Tracing Mapping Control flowcharting Job accounting data analysis System development life cycle System acceptance and control group

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

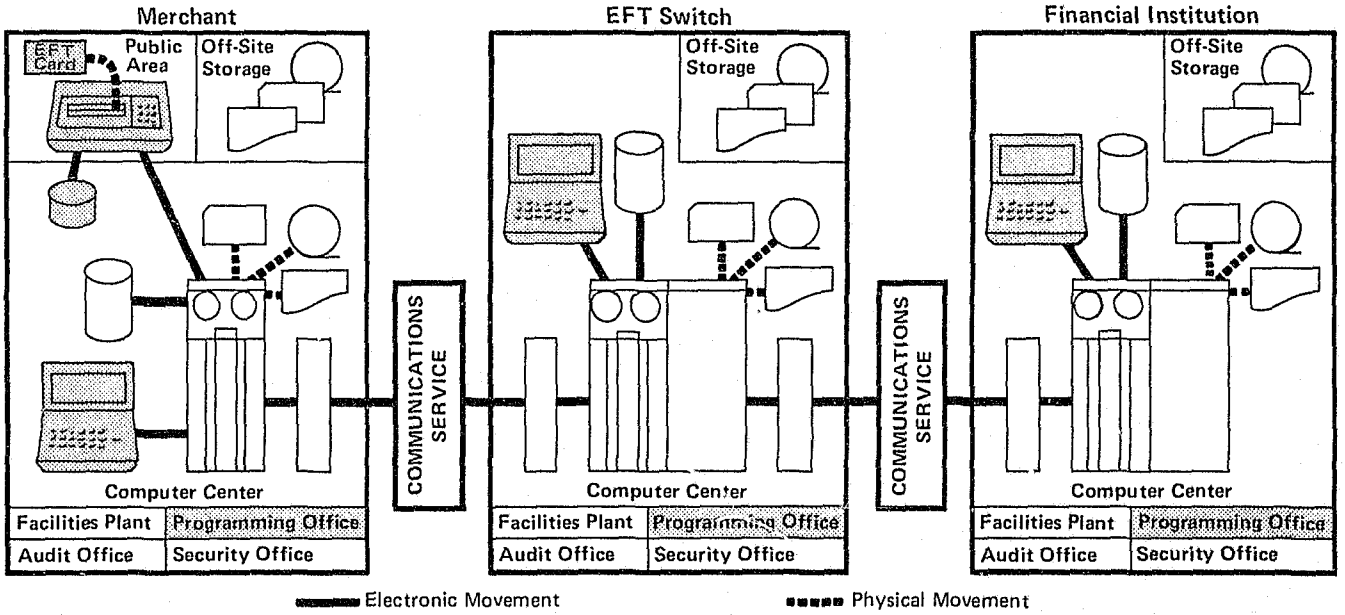
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



TERMINAL ENGINEER

Employers. Telephone company, maintenance vendor, product vendor.

Function. Terminal engineers test, diagnose, assemble and disassemble, repair, and replace EFT terminals or their components.

Important Knowledge:	Digital logic design Electromechanical engineering Communication engineering Boolean logic Terminal products
Important Skills:	Operation of terminals and electronic test equipment Electromechanical repair Reading circuit schematics and diagnostics manuals
Important Access:	On-line or off-line terminals and related communication equipment Test programs and test data Procedural documentation Work areas where terminals are located
Reports to:	Customer or maintenance management

Conclusions. Testing and equipment maintenance requires that terminal engineers function as transaction operators, but on a more privileged basis having access to more terminal commands than the transaction operator. When terminals are the intelligent variety with localized functions run by computer programs within the terminal, terminal engineers also have computer programming ability. They can cause a terminal to function in a supervisory or privileged access mode. These individuals are normally not employed by the EFT participant and are not under EFT management control. They are also free to come and go, and they are frequently familiar with the facilities and operations of a large number of EFT participants. They could gain a wide range of knowledge of EFT systems operations, including those among merchants, the EFT switch, financial institutions, and communications companies. Limitations of their knowledge of EFT systems files and central computer programs will limit their abilities to perform unauthorized acts. Their employer, the vendor company, should be required to assume accountability for the integrity, competence, and trustworthiness of each terminal engineer. This should be done with formal arrangements between the vendor and the customer.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, Programming, & Electronic: Use, modification, destruction, and taking of EFT terminal and communication equipment. Modification, destruction, and disclosure of computer programs and data files where access is made through terminals	**Object of:** Transaction origination Data communication Computer processing Data storage and retrieval Output processing **Responsible for:** Transaction entry	Transaction selection Embedded data audit collection Extended records Generalized audit software Snapshot Tracing System acceptance and control group Code comparison Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

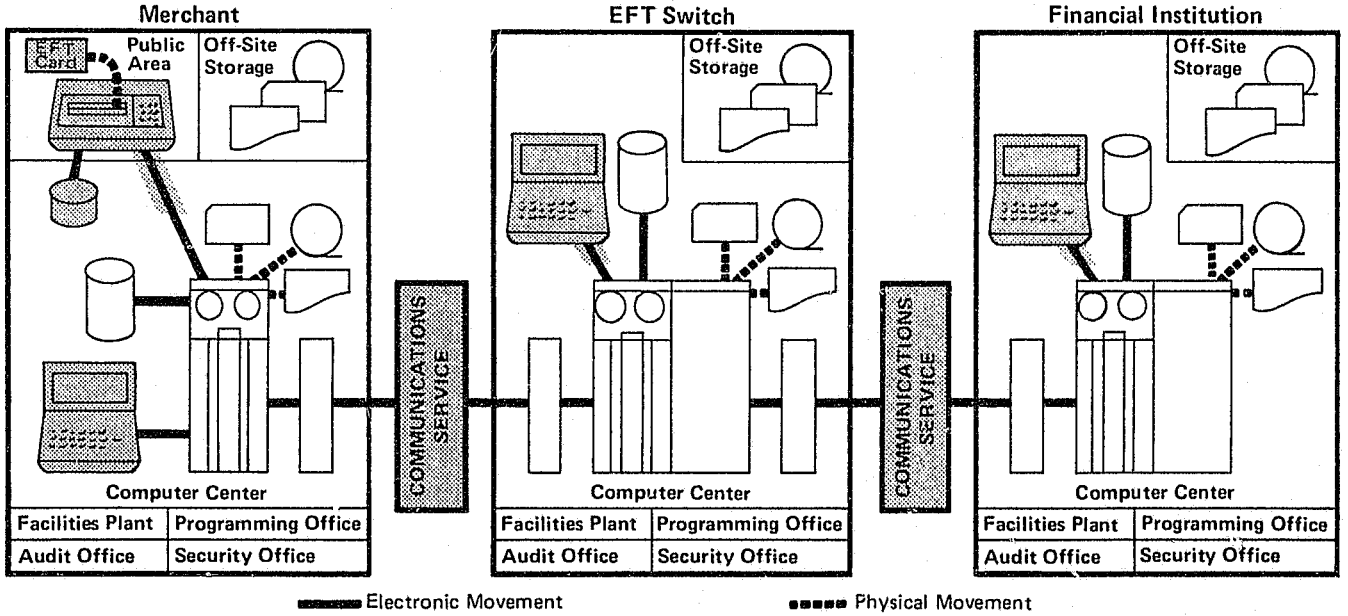
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



SYSTEM ENGINEER

Employers. Computer product vendor or maintenance vendor.

Function. The system engineer tests, diagnoses, assembles and disassembles, and repairs or replaces computer system hardware and components. Hardware includes computers, terminals, peripheral devices, and communication equipment.

Important Knowledge:	Digital logic Electromechanical engineering Communication engineering Programming Terminal protocol Physical access protocol Test equipment
Important Skills:	Terminal and computer console operation Communication equipment operation Peripheral operation Test equipment and tools operation Electronic and mechanical assembly and disassembly Reading memory dumps, circuit schematics and diagnostic manuals Computer systems programming
Important Access:	Test programs Data Operating system and circuit documentation
	All computer and peripheral equipment, Vendor's maintenance office, and surrounding and connecting facilities
Reports to:	Customer service management

Conclusions. These individuals are normally employed by the computer or maintenance vendor. They are not under management control of the EFT participants in whose organizations they are maintaining systems and components. This situation requires that the vendor ensure the integrity, competence and trustworthiness of the individuals. They frequently have access to more than one EFT participant. They are often knowledgeable of both hardware and software, and understand the computer operating system. Possible limitations of these individuals as a vulnerability include their lack of knowledge of the applications and data files content in the EFT system. These individuals usually cannot be effectively evaluated or audited by auditors or by any other technical people in the facilities in which they work. The best protection is to limit their facilities access, independently log their use and access to computer equipment and software, and ensure that no production or sensitive data remains in any storage devices where they are working.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, Programming & Electronic: Modification, destruction, disclosure, use and taking of computer and peripheral equipment, software, test equipment and test data.	**Object of:** Computer center **Responsible for:** Computer processing Data storage and retrieval Output processing	Test data method Base case system evaluation Integrated test facility Parallel simulation Embedded audit collection Extended records Generalized audit software Snapshot Tracing System acceptance and control group Code comparison Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

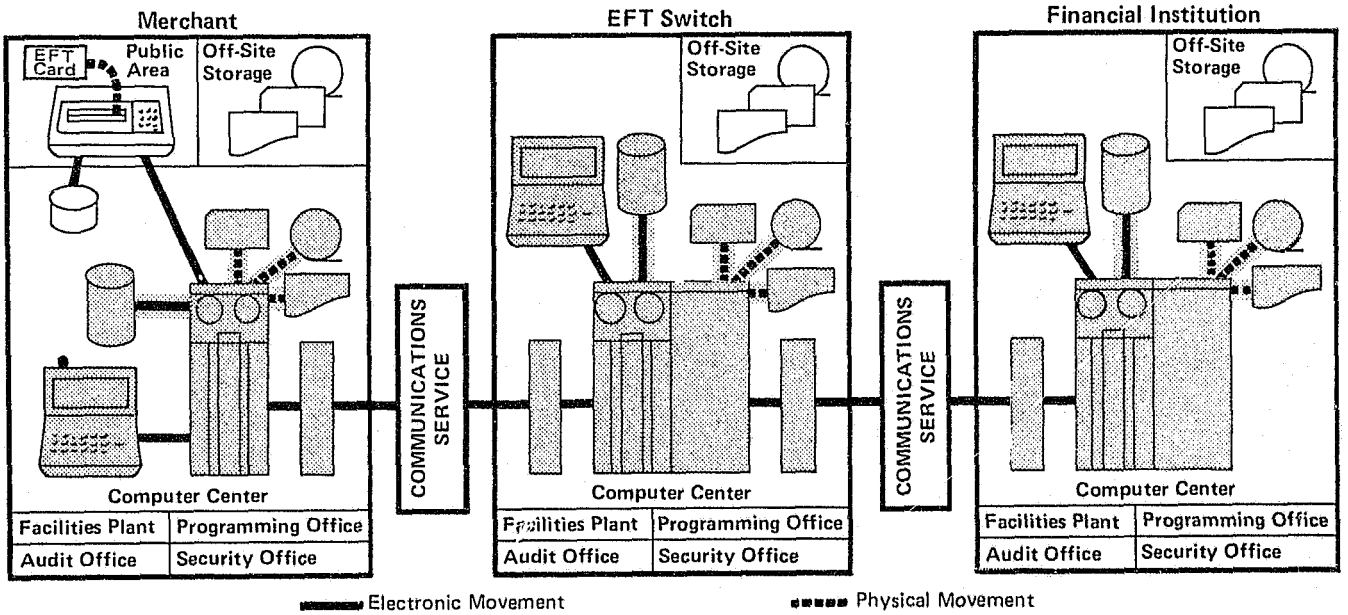
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



COMMUNICATION ENGINEER

Employers. Telephone company, product or maintenance vendor.

Function. The communication engineer tests, diagnoses, assembles and disassembles, repairs, and replaces data communication equipment and telephone circuits.

Important Knowledge:	Electronic and communication engineering Physical access procedures Data communication and Boolean logic concepts
Important Skills:	Operation of communication equipment and electronic test equipment Reading of circuit schematics and diagnostic manuals
Important Access:	Circuit and network diagrams Communication equipment and surrounding facilities
Reports to:	Customer service management

Conclusions. These individuals can modify or disclose data communicated through an EFT network. This vulnerability is minimized, however, because usually they have little knowledge of the meaning and content of the data transmitted. They could cause significant losses through destruction or unauthorized modification of communication equipment and circuits. The EDP auditor has minimal control or audit ability over the functions of these individuals since the auditor has little technical knowledge in this area. System and application program controls can be used to ensure the validity of messages transmitted and received, but they have no control over the disclosure of transmitted data through wiretapping or other listening methods. These individuals are employed by the vendor and are not under the management control of the EFT participant organization using their services. It is important for the participant to receive assurance from the vendor of the individuals' competence, integrity, and trustworthiness.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical & Electronic: Modification, destruction, taking and unauthorized use of communication equipment and transmission circuits	**Object of:** Transaction Origination Transaction entry Computer processing Output processing Computer center **Responsible for:** Data communication	Test data method Base case system evaluation Parallel simulation Transaction selection Embedded audit data collection Extended records Generalized audit software Snapshot Tracing System acceptance and control group Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

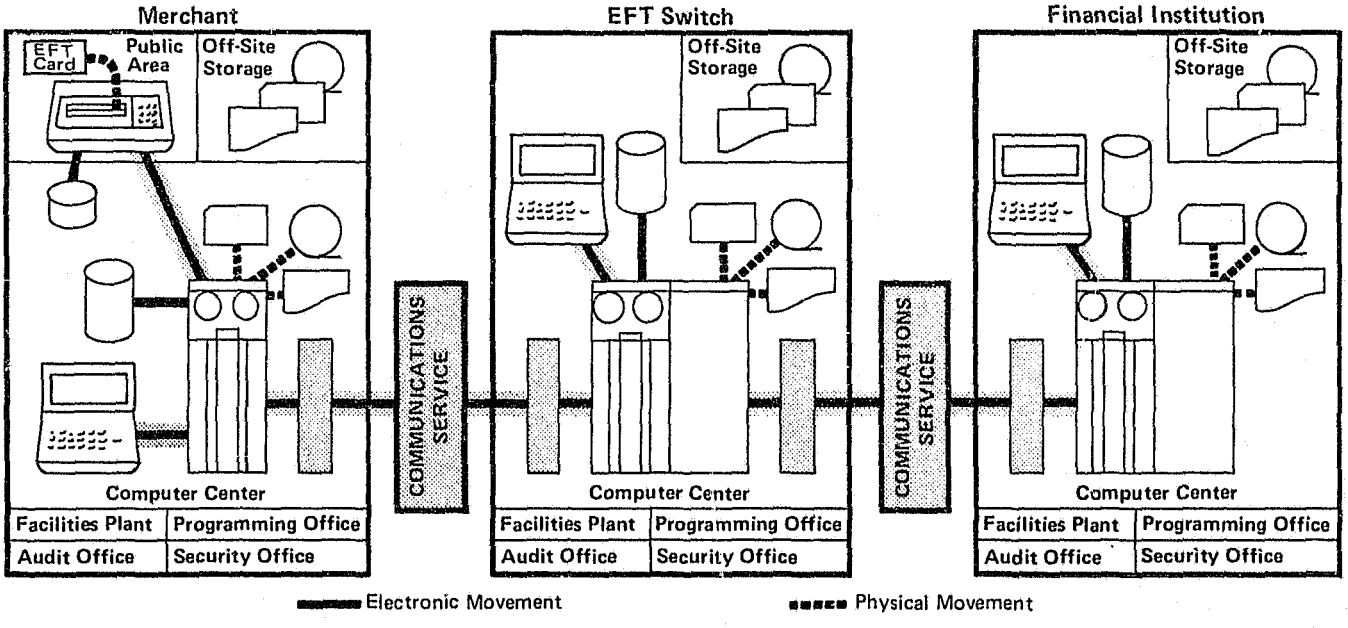
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



FACILITIES ENGINEER

Employers. Service or product vendor, maintenance contractor, EFT switch, merchant, financial institution, facilities management company and service bureau.

Function. The facilities engineer inspects, adjusts, repairs, modifies, or replaces equipment supporting computer and terminal facilities, e.g., air conditioning, light, heat, power, and water.

Important Knowledge:	Electromechanical engineering at the technician level
Important Skills:	Using test equipment and tools Reading building, circuit, and engineering schematics
Important Access:	Building and equipment diagrams and documentation All building facilities housing computer communication and terminal equipment Clerical and office areas Facilities environmental control equipment
Reports to:	Building management or customer service management

Conclusions. Computers, terminals, and communication equipment are highly susceptible to fluctuations in the air and power supplies. These individuals could be responsible for major and minor failures on a disaster or limited failure basis. Auditors have little knowledge of facilities equipment and would generally be incapable of reviewing these individuals' functions and activities. If they work for an outside vendor, assurance is needed as to their competence, integrity, and trustworthiness.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical: Modification, destruction or taking of facilities equipment, including air conditioning and utilities services. Causing air conditioning, backup power, and lighting failures	**Object of:** None **Responsible for:** Computer center	Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

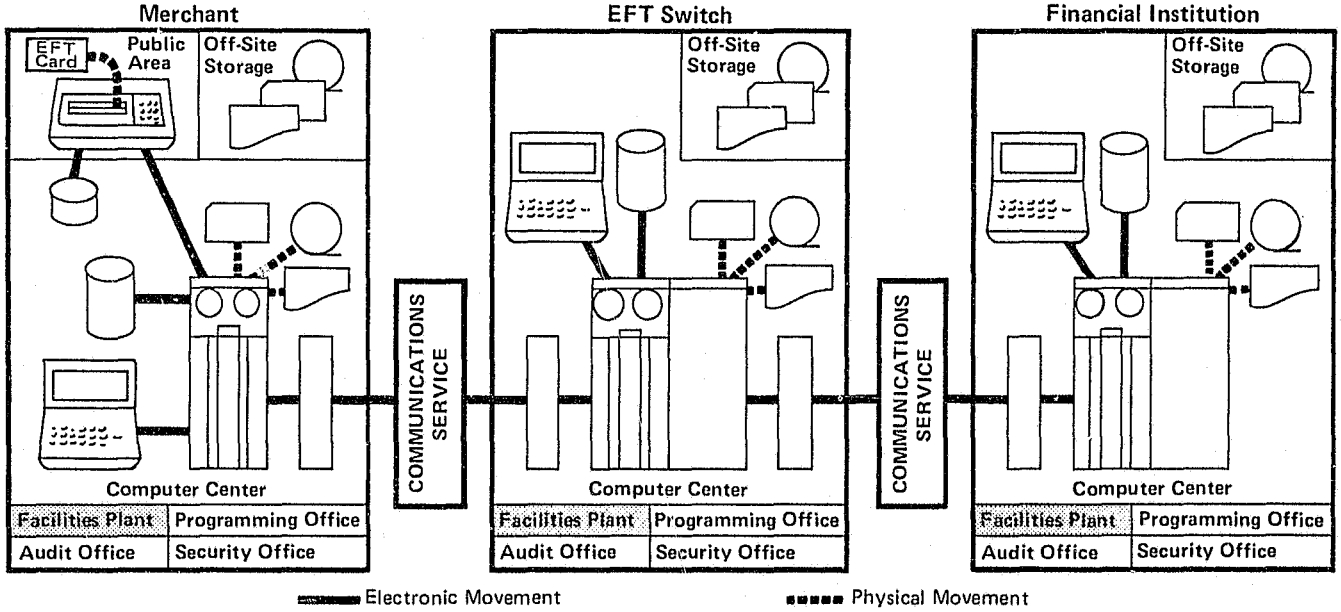
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



NETWORK MANAGER

Employers. EFT switch, financial institution, facilities management contractor, and service bureau.

Function. The network manager specifies and orders change, modification, addition, replacement, or elimination of functions and equipment in the communication network through directions given to subordinates.

Important Knowledge:	Communication and operating systems software Communication engineering Procedures for system integration Physical access Security and passwords EDP production workflow
Important Skills:	Management Interpretation and analysis of circuit schematics and diagnostics Systems analysis
Important Access:	Communication equipment and adjacent facilities Documentation including operating system, circuit, and network diagrams, and procedural manuals
Reports to:	EFT system management

Conclusions. They can make erroneous decisions that can have significant cost impact on the EFT network by selecting mismatched equipment and communication services related to the needs and performance requirements of the network. They can also make intentional decisions to place unauthorized EFT participants on the system network. The unauthorized participants could cause significant harm and losses to other participants. An unauthorized participant might be a financial institution or merchant controlled by organized crime or a foreign power intent on causing harm or making unauthorized gains.

These individuals also play a key role in recovering and restoring service when system failures occur or disasters are experienced. They should be familiar with documented contingency plans and be prepared to take appropriate action in case of such losses. Data communication controls and especially cryptographic protection are the most effective means of safeguarding against these individuals' unauthorized acts. They are, however, able to compromise cryptographic hardware or software. Auditors usually must put great trust in these persons since the auditors do not have the technical expertise to detect wrongdoing or many possible errors and omissions.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Programming, & Electronic All threats posed by communications engineers and to some extent systems engineers	**Object of:** Transaction origination Transaction entry Computer processing Computer center **Responsible for:** Data communication	Test data methods Base case system evaluation Parallel simulation Transaction selection Embedded audit data collection Extended records Generalized audit software Snapshot Tracing Control flowcharting Job accounting data analysis

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

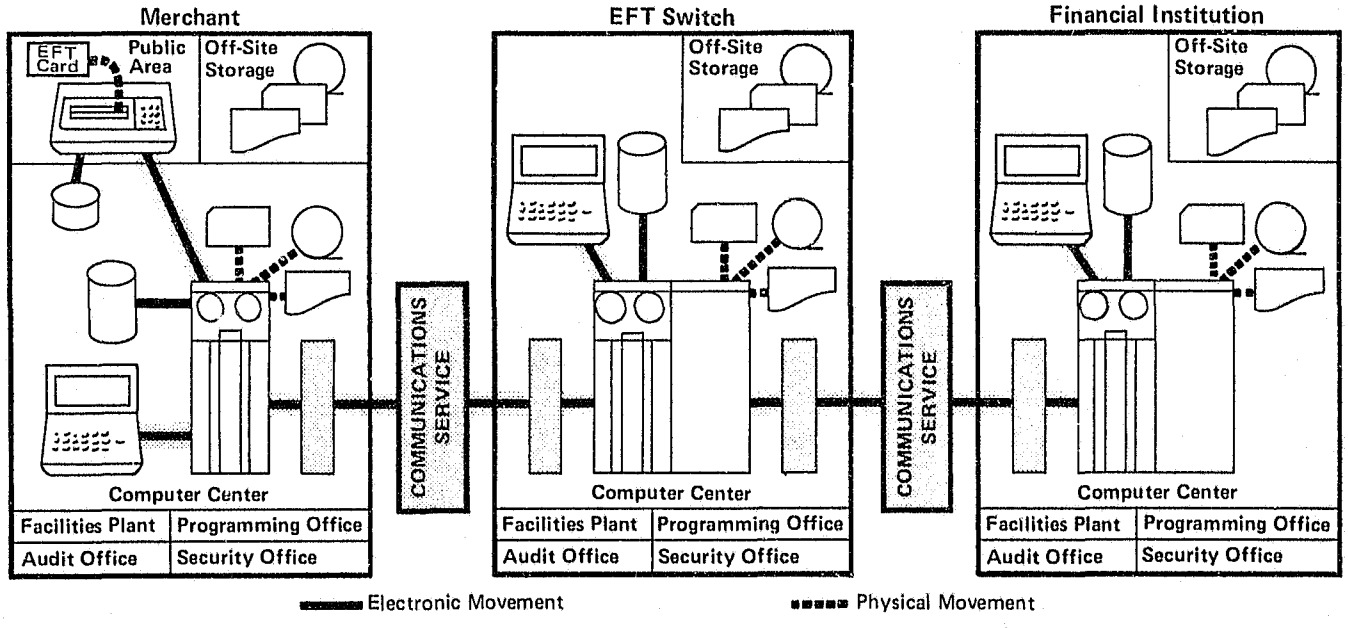
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



OPERATIONS MANAGER

Employers. Merchant, financial institution, EFT switch, facilities management contractor and service bureau.

Function. The operations managers change modify, add, replace, and eliminate processing steps in the computer production workflow through direction given to operational subordinates. If system programming is within their area of responsibility, they can also change, modify, add, replace or eliminate functions in the operating systems software through direction given to systems programmer subordinates. They also are responsible for security of the equipment facilities and operations. They may have authority to assign or change terminal and facilities access control passwords.

Important Knowledge	Computer operating system and utilities software Operations procedures for data files Media library Job accounting System integration and maintenance Physical access Security Workflow
Important Skills:	Reading flowcharts and procedural documentation Performing systems analysis Management Principles of operation
Important Access:	Operating system Data files Procedural documentation All computing equipment and facilities Job input-output Scheduling and servicing areas Media library and its content
Reports to:	EDP management

Conclusions. Because these individuals are responsible for most of the controls in the computer operating system and in computer operations, they can easily violate most of the controls. When they manage the systems programming staff, they often are not sufficiently technically skilled to validate and check the work being performed by the systems programmers. Through errors and omissions they can cause significant losses. They are also in a position to direct unauthorized activities of computer operations and systems programming staffs. Auditors are usually able to detect major unauthorized acts performed in the computer operations area. Generalized audit software would have to be run independently of the computer operations staff to be effective in auditing these individuals. Parallel simulation in a different computer center would be effective if not under the control of operations managers.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, & Programming: Similar to systems programmer and computer operator. Through this management position they are able to direct technologist subordinates to engage in erroneous or intentional acts that could result in losses	**Object of:** Data communications Computer processing Data storage and retrieval Output processing **Responsible for:** Computer center	Test data method Base case system evaluation Parallel simulation Transaction selection Embedded audit data collection Extended records Generalized audit software Control flowcharting Job accounting Data analysis System development life cycle Code comparison Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

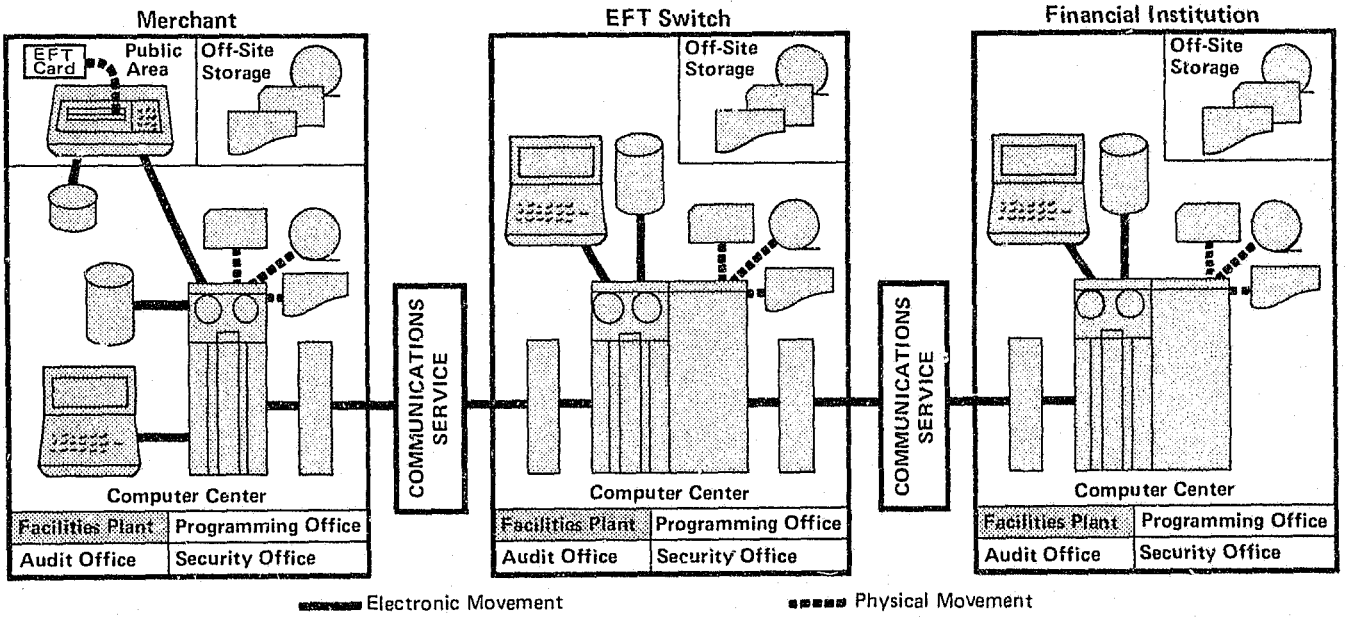
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



DATA BASE MANAGER

Employers. EFT switch, financial institutions, facilities management contractor, and service bureau.

Function. The data base manager changes, modifies, adds, replaces or deletes records in on-line and off-line data bases through direction given to subordinates.

Important Knowledge:	Data base software Procedures for data file handling Media library Job accounting System integration Testing application program functions and data base structures Interfacing with other functions
Important Skills:	Reading flowcharts and diagrams Performing systems analysis Reading procedural documentation
Important Access:	Data base storage areas EDP production workflow Security and passwords
Reports to:	Operations manager

Conclusions. These individuals have transaction access to the production data files and direct subordinates in these activities. Because they are responsible for correction of errors and omissions in data files, they represent a significant vulnerability. These individuals cannot, however, effectively modify computer programs. Logging and detection controls on their activities can be particularly effective. Their actions can be controlled only if the auditor has the same skills and knowledge as a data base manager.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical & Transactional: Modification, disclosure and destruction of data bases. Unauthorized use of utility programs.	**Object of:** Transactions entry Computer processing Data storage and retrieval Output processing Computer center **Responsible for:** Data storage and retrieval	Transaction selection Embedded audit collection Extended records Generalized audit software Snapshot Control flowcharting Jobs accounting Data analysis

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

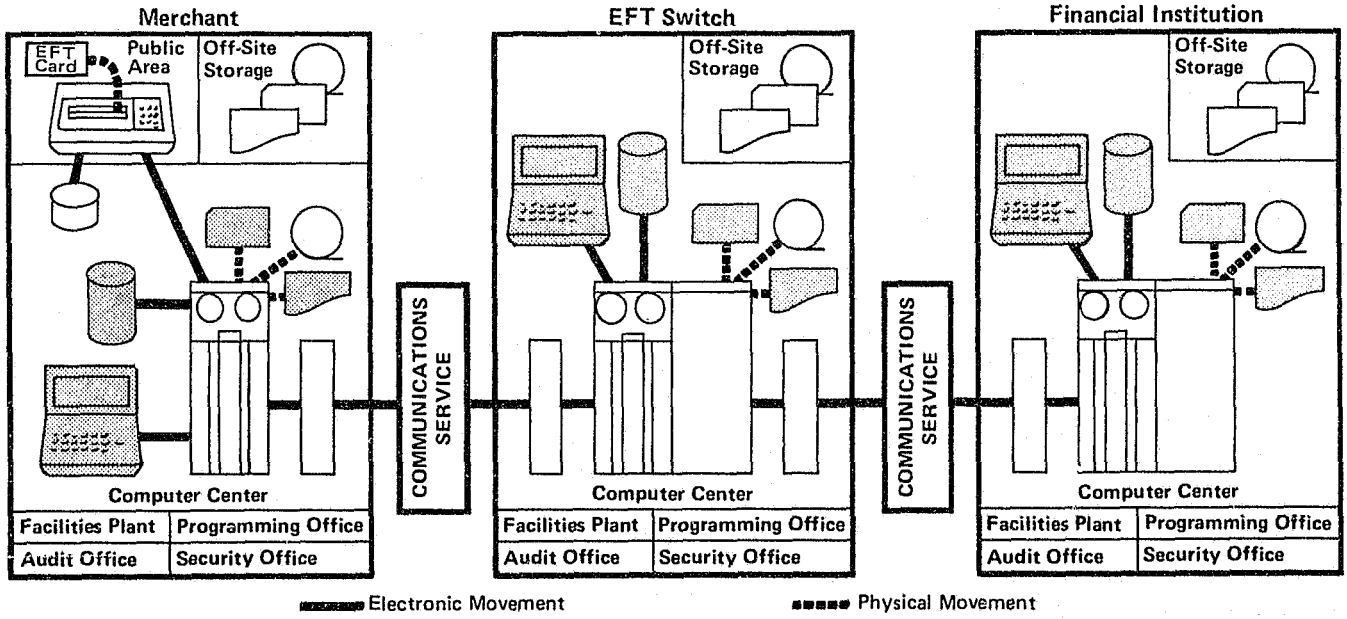
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



PROGRAMMING MANAGER

Employers. Merchant, EFT switch, financial institution, facilities management contractor, and service bureau.

Function. The programming manager changes, modifies, adds, replaces, or eliminates application programs or parts of application programs through subordinates.

Important Knowledge:	Application programming languages Application subject areas such as accounting and demand deposit services Structured programming and software engineering concepts Procedures for data base design Programming library Job accounting System testing and integration Physical access Security Computer production workflow
Important Skills:	Reading flowcharts Program listings Program documentation Systems analysis Management Programmer performance evaluation
Important Access:	Application programs and documentation Program library Programming procedures Programmer offices and work areas Computer production user areas Offices
Reports to:	EDP management

Conclusions. These individuals present the same vulnerabilities that application programmers pose. However, the programming managers have a wider knowledge and control across applications and parts of application programs. They are able to integrate unauthorized changes across wider ranges of applications. They are also able to take computer programs for use by unauthorized individuals and develop new application programs using their employer's computer for unauthorized purposes. They are responsible for implementation of most controls that are part of the application programs. Computer center controls to limit their access to computer production runs and the system acceptance and test function are the most effective to ensure prevention and detection of unauthorized activities. The auditors must work closely with these individuals to ensure adequate controls in application programs. They do not have access to the computer operating system software or hardware which limits their unauthorized activities to the modification of computer programs in the application area.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, & Programming: Modification, destruction, use and disclosure of computer program applications, documentation, and test data.	**Object of:** Computer center **Responsible for:** Transactions origination and entry Data communication Computer processing Data storage and retrieval Output processing Application System development	Test data method Base case system evaluation Integrated test facility Parallel simulation Extended records Generalized audit software Snapshot Tracing Mapping Control flowcharting Job accounting data analysis System development life cycle System acceptance and control Code comparison

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hip diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

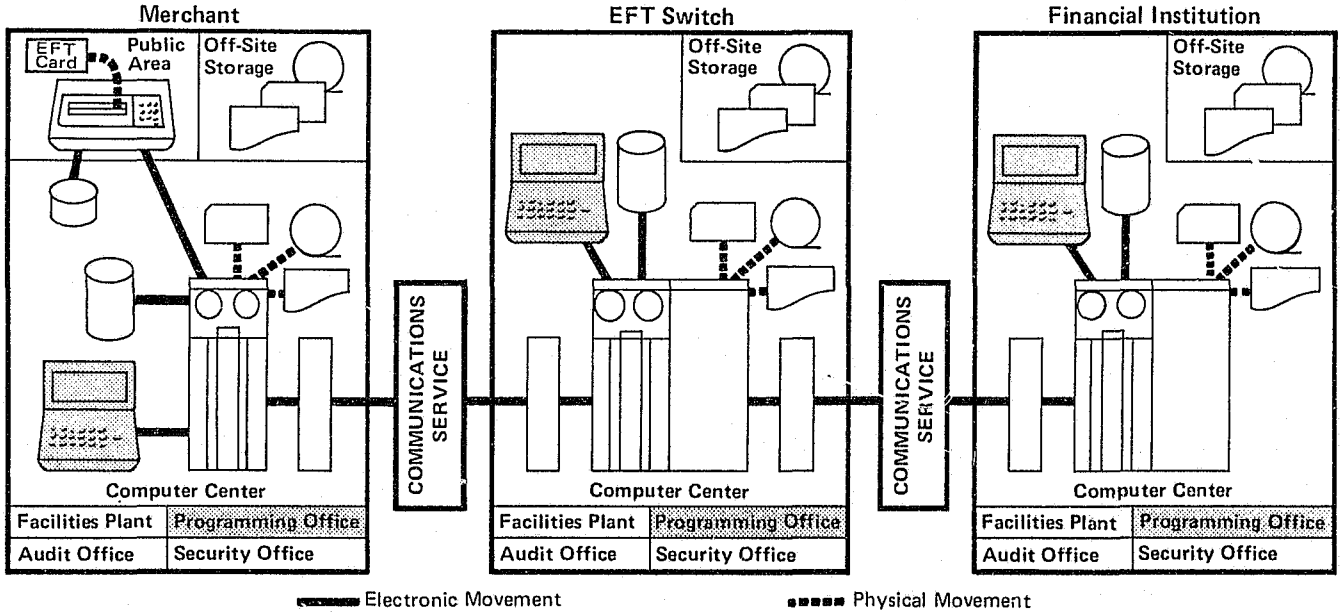
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



IDENTIFICATION CLERK

Employers. Financial institution and service bureau.

Function. The identification clerk assigns account numbers and issues personal identification numbers and devices; releases batches of data for the production, embossing and encoding of EFT plastic cards and other identification materials; terminates accounts and personal identification of former customers.

Important Knowledge:	Customer data file organization Identification workflow procedures
Important Skills:	Terminal keyboard input and operation Plastic card embossing/coding equipment Reading identification listings and procedural documentation
Important Access:	Computer terminals Identification files and materials work areas Production control area Output receiving area
Reports to:	Operations management

Conclusions. The greatest vulnerabilities from these individuals are credit card fraud and other impersonation and counterfeiting activities. The most effective controls are those concerned with the accounting of identification materials and inventory control of such materials.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical: Modification, disclosure and destruction of personal identification materials and personal identification information, including plastic cards, pin numbers, and computer output listings of personal identification Modification, destruction, and disclosure of personal identification data in computer storage files	**Object of:** Transaction origination Computer processing Data storage and retrieval Output processing Computer center **Responsible for:** None	Transaction selection Embedded audit data collection Extended records Generalized audit software Job accounting data analysis Disaster testing

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

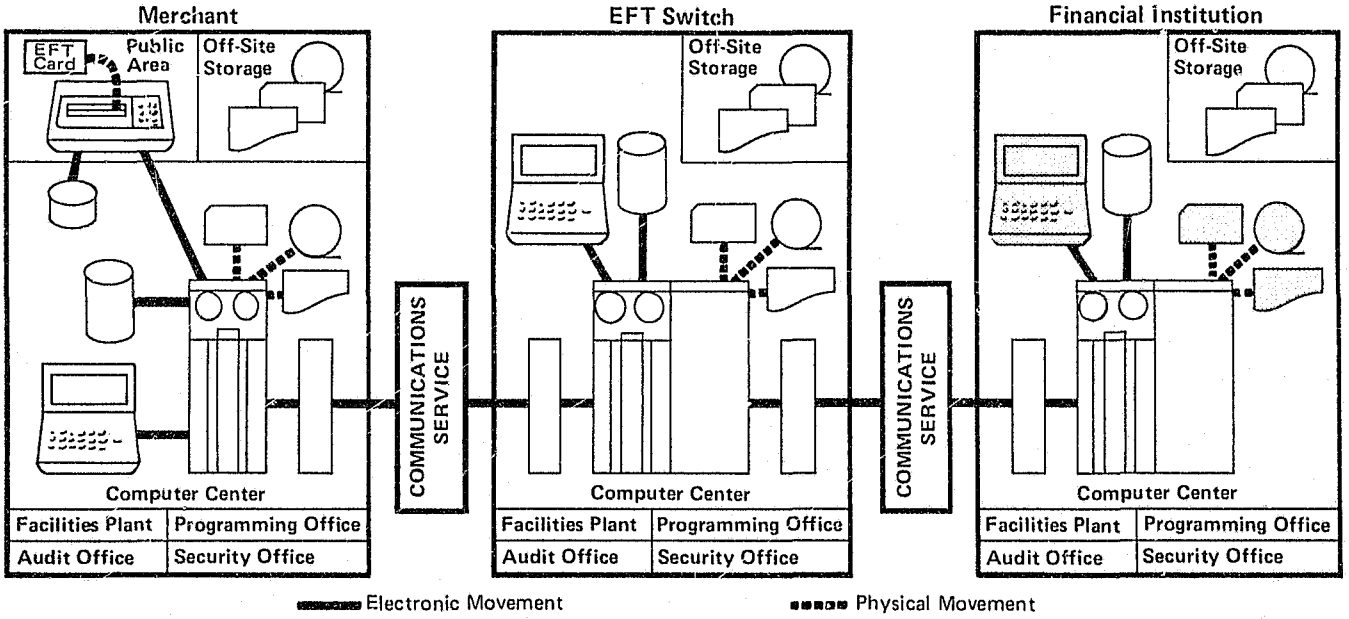
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



SECURITY OFFICER

Employers. Merchant, EFT switch, financial institutions, facilities management, contractor, service bureau, and communications supplier.

Function. The security officer evaluates, plans, implements, operates, and maintains physical, operational, procedural, personnel, and technical safeguards and controls.

Important Knowledge:	Industrial security products and practices EDP Software and hardware technology Procedural, operational, and personnel policy and practices Security Identification administration
Important Skills:	Electronic Mechanical Programming technician capabilities Reading mechanical, building, electronic, and programming schematics
Important Access:	Privileged access to all areas
Reports to:	Data processing management

Conclusions. Since these individuals have privileged access to all areas and have knowledge of all functions and activities, audit is limited to operational security reviews and ensuring adequate trustworthiness of the individuals through background and performance evaluation. Although all vulnerabilities are present, the individuals often do not have sufficient depth of knowledge and skills to perform unauthorized acts without being detected (especially by personnel specialized in the area of the unauthorized activity).

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, Programming & Electronic: All vulnerabilities present	**Object of:** None **Responsible for:** All controls	None

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

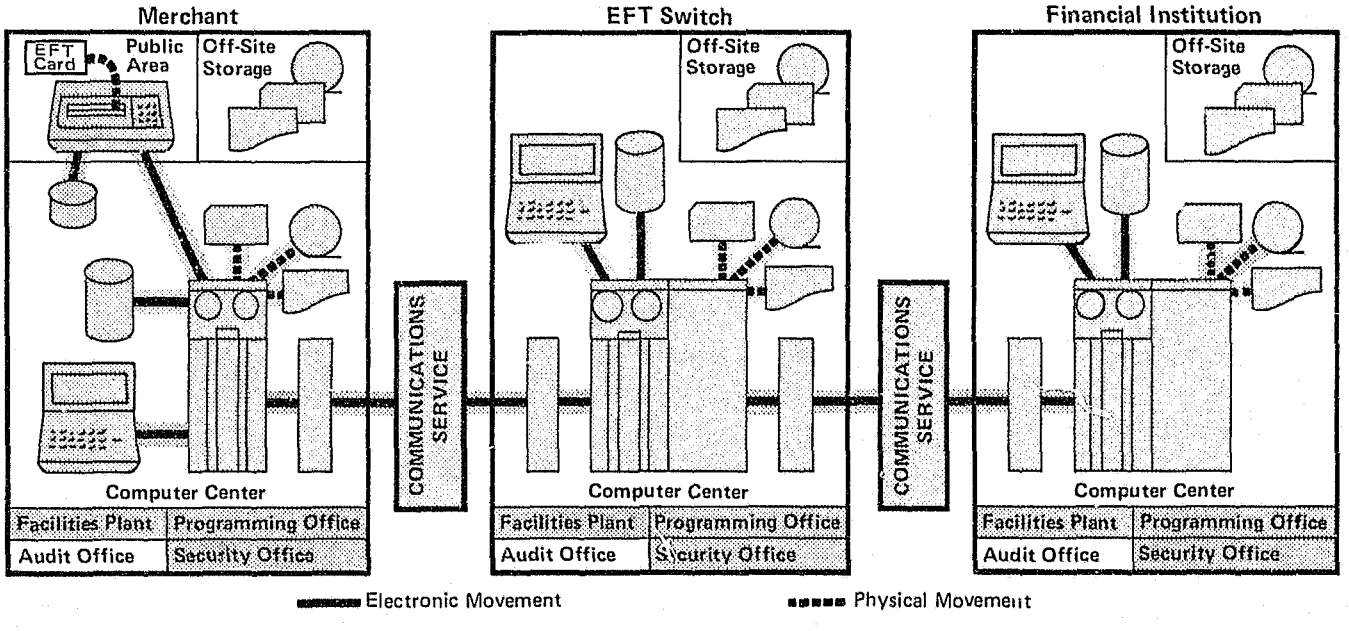
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



EDP AUDITOR

Employers. Merchant, financial institution, EFT switch and service bureau.

Function. The EDP auditor performs operational, software and data file reviews to determine integrity, adequacy, performance security, and compliance with organization and generally accepted policies, procedures, and standards; participates in design specifications of applications to ensure adequacy of controls; performs data processing services for auditors.

Important Knowledge:	Audit techniques Controls Safeguards Computer applications Software organization System design Facilities Security
Important Skills:	Use of audit tools Programming Reading operational and technical documentation
Important Access:	Privileged access to all areas
Reports to:	Highest level of management

Conclusions. EDP auditors are in positions of total trust. Trustworthiness can be evaluated through background screening and performance by external CPA auditors and examiners from regulatory agencies. Some protection is available through peer review of the individuals' work and activities. Also, the auditor tends not to have sufficient knowledge and skills to perform unauthorized acts that could go unnoticed by personnel in the areas of the authorized acts.

Vulnerabilities	Controls	Audit Tools & Techniques
Physical, Transactional, Programming & Electronic: All unauthorized acts are possible.	**Object of:** None **Responsible for:** All controls	None

VULNERABLE AREAS

(Unshaded areas are not considered probable vulnerabilities for this occupation.)

KNOWLEDGE

Software
- Application/data base programs/ language
- Operating system/communications/ utilities
- Modeling/simulation

Hardware
- Digital logic design
- Electronic/electro-mechanical engineering
- Communication engineering

Procedures
- Programmer terminals protocol
- Remote point-of-transaction terminals
- CPU console protocol
- Data file/library/job accounting
- System integration/testing/interfaces
- Physical access
- Security/identification
- EDP production workflow
- Authorization limit controls
- Account number standards

Concepts
- Accounting
- Data base/data communications
- Computer architecture
- Boolian logic
- Structured design/programming
- Inventory control

SKILLS

Operational
- Terminals/keyboard
- CPU console
- Communication equipment
- Peripheral equipment
- Microfilm/microfiche equipment
- Electronic test equipment/tools
- Electronic fabrication
- Plastic card embossing/encoding equipment
- Record keeping/filing

Interpretive/Analytical
- Read memory dumps
- Read flow charts/hipo diagrams
- Read circuit schematics
- Read diagnostic/error codes
- Convert binary to character
- Write logical expressions
- Draw flow charts/diagrams/ circuits
- Perform systems analysis
- Read procedural documentation

FUNCTIONAL ACCESS

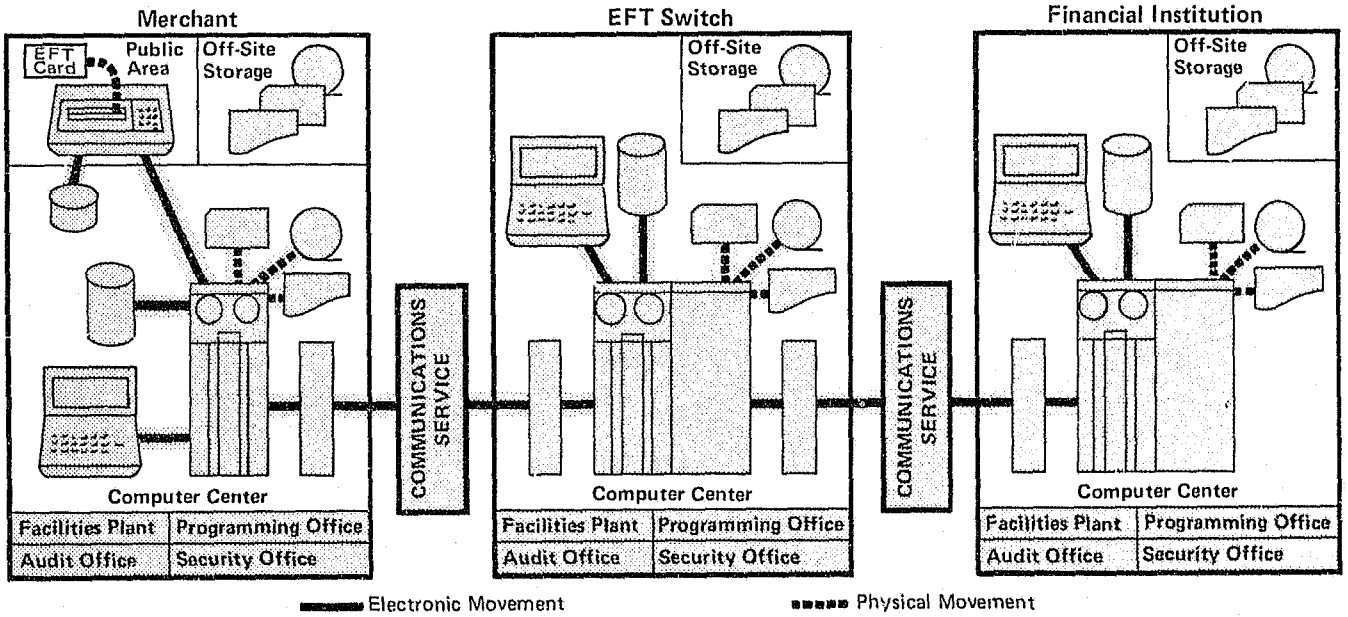
Data files
- Application program library
- Accounts/master files
- Transactions/file update data stream
- Security codes
- Operating system programs
- Testing programs/data
- History files off-line/on-site
- Remote storage

Documentation
- Operating system/sysgen
- Application programs/data layouts
- Data base structure
- Circuit/network diagrams
- Procedures

Hardware
- Computer equipment
- Communication equipment
- Programmer terminals
- Remote terminals
- Facilities equipment/power, air conditioning
- Personal identifiers

Production Control
- Job set-up
- User output

PHYSICAL ACCESS



IX CONCLUSIONS

EDP and EFT security is principally a people problem. Security vulnerabilities are primarily derived from the potential activities of data processing employees. Twenty occupations, each with a specialized set of skills, knowledge, and access have been identified as being in high positions of trust requiring controls and auditing. The occupations are also found among most EFT participants. Exceptions are the telecommunications companies, service companies, product vendors, and external auditors where few of the identified occupations are found.

Basic concepts of security encourage increasing the trustworthiness and reliability of EDP personnel and controlling the degree of trust that must be placed with them. This can be done most effectively by:

- Helping satisfy the personal needs of employees to reduce the possibilities of temptations to violate their trusts.
- Applying controls and audit.
- Making such employees sensitive to the need for security.
- Causing employers to have more personal, detailed information about their employees and prospective employees in matters that relate to the employees' positions of trust.

Vulnerabilities — The vulnerabilities are both accidental and intentional acts performed by people in the 20 occupations (based on studies of computer abuse and misuse conducted by SRI International over the last seven years). These two kinds of vulnerabilities are quite different in important respects. These differences require divergent kinds of strategies for security, but this guide describes only controls and audit tools and techniques that apply to both kinds of vulnerabilities.

Among the four classes of vulnerabilities (physical, transactional, programming, and electronic), physical types of acts occur among all occupations. They are related to physical and functional access as described in the occupation descriptions. Vulnerabilities derived from programming and electronic manipulation are usually not found among the clerical and operational occupations because people in these occupations do not have sufficent skills, knowledge, and access to perform these more technical and sophisticated acts. In fact, electronic manipulation is even more narrowly limited to terminal and systems maintenance engineers and equipment vendors' representatives.

It is important to note that security officers and internal EDP auditors are able to perform acts covering the entire range of vulnerabilities. This ability is derived from the full range of skills, knowledge, and physical and functional access they possess for their occupations. The only people usually able to apply detection and prevention controls to these two occupations are the external auditors and examiners. It is important that management, CPA firms, and regulatory agencies recognize the vulnerabilities represented by security officers and internal EDP auditors and ensure that proper controls are applied.

Controls and Audit Tools and Techniques — Most of the eight categories of controls identified in this guide include physical controls or controls of physical vulnerabilities. Only two types of controls apply to the electronic class of vulnerabilities:

- Data storage and retrieval controls assist in ensuring that the electronic maintenance engineers do not have access to sensitive files of data.
- Computer center controls are meant to include means of controlling physical access of the maintenance engineers.

Only two types of controls apply to systems and applications programmers — computer center and application system development. These are most important because programmers are in the greatest positions of trust. Because of the complexity of their work, detection of unauthorized or erroneous activities is limited.

Most audit tools and techniques are meant to apply to programming and electronic vulnerabilities. Only a few apply to transaction and physical vulnerabilities. Parallel simulation, job accounting data analysis, and disaster testing apply to physical vulnerabilities because these tools and techniques are concerned with manual and operational functions of EDP personnel. Audit tools and techniques are effective against programming and electronic vulnerabilities because most can be applied without programmer or engineer involvement.

In general, EDP controls in computer programs are less effective against programming and electronic vulnerabilities. This is because controls in software can easily be compromised by intentional programming and electronic acts and are ineffective against people with these skills. Although

many controls apply to the more technically sophisticated acts, controls are usually more effective for the less technical occupations. This anomaly indicates a need for the development of new and more effective controls for acts perpetrated by programmers and engineers. Controls that affect the widest range of occupations are those controlling procedural activities among EDP personnel. It cannot, however, be assumed that controls affecting smaller numbers of occupations are less valuable. For example, application system development controls affect the fewest number of occupations, but because this type of control is the only one applicable to application programmers, it is extremely important in this one area.

Although no controls have been identified as effective for facilities engineers, security officers, and EDP auditors, the latter two are identified with the largest number of vulnerabilities. This puts these two occupations in high positions of trust relative to the types of vulnerabilities associated with them. Next in fewest number of applicable control types are application programmers, systems programmers, systems engineers, and programming managers. Systems programmers may be in a higher position of trust than application programmers because of the wider range of access but their lack of knowledge of applications may tend to reduce this position of trust somewhat.

Occupational Access — Analysis of occupations and functional access indicates that remote backup storage files, the application program library, security code files, application program documentation, and building equipment (such as that used for air conditioning, power, and heat) should all have the least number of different types of employees with access. Remote backup storage files and the security code files should have minimum numbers of people with access. Physical access controls should be used to ensure that employees do not enter areas where there is no functional need. In particular, computer facilities should be laid out in a building to minimize the need for employees to pass through other functional areas on the way to their own work areas. The media library should have the fewest number of employees having access and should be limited to media librarians and operations managers. This is one of the more difficult access controls to apply to smaller computer installations in which computer operators must directly obtain magnetic tapes for use on the computer. The backup storage site is the next area requiring the least number of people having access. Only employees carrying materials from the computer facilities to the backup storage areas need have access to it.

Skills and Knowledge — It is clear that fewer numbers of technical skills are required among the operational occupations and management. The greater number of skills are necessary for programming, systems engineering, security, and audit occupations. Technical knowledge is similarly greatest among the programming, managerial, security, and audit occupations and least among the operational occupations. The need for knowledge of physical access controls and security identification is quite universal among the occupations. Employees must be aware of areas they are not allowed to enter in computer facilities. They must also have adequate knowledge of necessary passwords and access devices to perform their work.

With the advancing use of computer technology and electronic funds transfer, data worth billions of dollars are stored and processed in computer and data communications systems. These data are vulnerable to error prone and unscrupulous people. If those assets were in physical form, they would be stored in time-locked vaults and would be processed and moved under the watchful eyes of guards. The needs of automation preclude this type of safeguarding, but we do not yet know how to provide equivalent protection in automated systems. Not enough resources are being expended to achieve the needed controls and audit tools and techniques. Fortunately, the potential for sufficient protection at reasonable cost does exist in the use of computers. That potential should be developed.

OTHER PUBLICATIONS IN THIS SERIES

The following is a list of additional FDIC publications on EFT. Copies may be obtained from:

Division of Management Systems and Financial Statistics
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429

Introduction to Point of Sale Systems — February 1976

Introduction to EFT Security — August 1976

Introduction to Automated Tellers — November 1975

Introduction to the Automated Clearing House — November 1976

Glossary of Acronyms and Terms (September 1975) is not currently available. It is being revised and will be available in early 1978.

END