12-1989

Electronic Data Processing and the Internal Control Structure

Mitch Byrne

UNIVERSITY OF NORTH DAKOTA

ELECTRONIC DATA PROCESSING AND THE INTERNAL CONTROL STRUCTURE

A RESEARCH PAPER SUBMITTED TO

DR. HANS JOHNSON

IN FULFILLMENT OF INDEPENDENT STUDY

DEPARTMENT OF ACCOUNTING AND BUSINESS LAW

BY

MITCH BYRNE

GRAND FORKS, NORTH DAKOTA

DECEMBER 1989

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The objectives of this report will be to describe the recommended procedures to be performed by an independent auditor in the auditor's study and evaluation of electronic data processing (EDP) accounting controls as part of the overall review of the accounting control system.

The second standard of field work states, "There is to be a proper study and evaluation of the existing internal control as a basis for reliance thereon and for the determination of the resultant extent of the tests to which auditing procedures are to be restricted."[1] This report will look at the study and evaluation of accounting control in accounting systems that include EDP activities. Planning for data-processing accounting control reviews should be coordinated with other audit plans and objectives.

Electronic data-processing systems usually eliminate the need for certain manual procedures and may create a need for others. An EDP system often consolidates several functions that were previously segregated in manual systems.

---

[1]AICPA, U.S. Auditing Standards, Vol. A (Chicago: Commerce Clearing House, Inc., 1988): 2147, section 320.01.

The elimination of some manual procedures and centralization of functions tends to combine incompatible functions within EDP, that is, it provides the ability both to commit and conceal errors or irregularities.[2]

The AICPA states if adequate accounting controls are to be maintained, it is necessary to implement compensating controls such as independent document counts, control totals of significant data fields, and control over access to EDP equipment and computer files. When these compensating controls exist, the system may well provide better and more consistent control than could be obtained in a non-EDP system.

Accounting Control

Accounting Control comprises the plan of organization and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records and consequently are designed to provide reasonable assurance that:[3]

A. Transactions are executed in accordance with management's general or specific authorization.

B. Transactions are recorded as necessary (1) to permit preparation of statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and (2) to maintain accountability for assets.

---

[2]AICPA, The Auditor's Study and Evaluation of Internal Control in EDP Systems, (New York: AICPA, 1977): 2.

[3]AICPA, Study of Internal Control in EDP Systems, 3.

C. Access to assets is permitted only in accordance with management's authorization.

D. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

The objectives and essential characteristics of accounting control do not change with the method of data processing. However, organization and control procedures used in electronic data processing may differ from those used in manual or mechanical data processing.

When reviewing controls in an accounting system, the auditor should develop an understanding of the flow of transactions through that system. When manual processes in an accounting system have been automated, the auditor should understand the transaction flow through both manual and EDP processing.

Description of EDP Activities

Business transactions include exchanges with parties outside the business entity and transfers or use of assets or services within the entity. These transactions can be recorded by manual or mechanical means, by EDP equipment, or by a combination of these techniques. In a manual system, transactions are typically supported by some kind of accountability, such as perpetual inventory records. Similar records often exist in an EDP system, but in some cases may be available only in machine-readable form.

Machine-readable data files frequently are the basic records of an EDP-based accounting system. These records ordinarily cannot be read or changed without the use of a computer. It is possible to alter these files without leaving any visible evidence of the change. Detecting a change in manual records is often difficult, but this difficulty can be greatly increased when dealing with possible changes in machine-readable records.

An EDP-based system includes the following elements:[4]

1. Hardware
2. Software
   A. System programs
   B. Application programs
3. Documentation
4. Personnel
5. Data
6. Controls

From the auditor's viewpoint, there are several significant differences between EDP activities and non-EDP activities. The remaining chapters will discuss these differences when using EDP in an accounting system. Chapter two will look at the auditor's review and evaluation of internal control of an accounting system using EDP.

Chapters three and four will discuss the general

---

[4]Ibid., 5.

controls and application controls for an EDP system. Chapter five will look at the auditing techniques which auditors use to audit through the computer to test EDP applications such as audit software, test data, and parallel simulation. Chapter six looks into the unique characteristics of specific EDP systems that are commonly found in the business environment such as batch processing, online processing, and small computer environment.

CHAPTER 2

AUDITOR'S REVIEW AND EVALUATION OF INTERNAL CONTROL

The essential characteristics of internal accounting controls include:[5]

1. Qualified and properly trained personnel.
2. Proper segregation of functions.
3. Execution of transactions by authorized personnel.
4. Accurate recording of transactions.
5. Access to assets limited to authorized personnel and to someone other than those who authorized transactions and record transactions.
6. Periodic comparison of recorded accountability with assets.

This chapter describes the application of this standard to the study and evaluation of internal accounting control for computer data processing.

The study and evaluation of internal accounting control can be divided conceptually into four steps, but for reasons of efficiency and effectiveness, these steps may not

---

[5]Taylor, Donald H., Auditing: Integrated Concepts and Procedures, (New York, N.Y., John Wiley & Sons, 1988): 407.

remain operationally distinct.[6]

1. Preliminary phase of the review.
2. Completion phase of the review.
3. Tests of Controls.
4. Evaluation of the system.

Preliminary Phase of the Review

The preliminary phase of the review of the client's system of accounting control provides the auditor with information about the computer data processing system so the auditor can decide how to proceed with the audit.

"The preliminary phase of the auditor's review should be designed to provide an understanding of (a) the flow of transactions through the accounting system, (b) the extent to which EDP is used in each significant accounting application, and (c) the basic structure of accounting control."[7] Thus the preliminary phase has three products:[8]

1. General understanding of the data processing system for accounting records.
2. General understanding of the extent to which EDP is used in significant accounting applications.

---

[6]Davis, Gordon B., Auditing & EDP, (New York: AICPA 1983): 28.

[7]AICPA, Study of Internal Control in EDP Systems, 10, citing AICPA, Statement on Auditing Standards No. 3, "The effects of EDP on the Auditor's Study and Evaluation of Internal Control," (New York: AICPA, 1974), paragraph 25.

[8]Davis, Auditing & EDP, 29.

3. Outline of the basic structure of accounting control for EDP as reflected in general controls and application controls.

General Understanding of the Data Processing System

To determine the scope of audit procedures related to computer processing, the auditor must consider the scope for the review of general controls and the applications to be reviewed and tested. The determination of scope requires a general knowledge of the computer data processing system and the applications for which the computer is used. This background information is obtained by the auditor as part of the survey of a new client's organization and organizational functions or the review of changes in an existing client's organization and functions.

The auditor obtains a general understanding of the data processing system for accounting records by identifying each significant class of financial transactions and reviewing the flow of these transactions as they are processed by EDP and non-EDP procedures. The auditor may gather information by the following methods of inquiry and discussion; observation; review of documentation and reports; and examination of transaction flows.[9] The resulting general understanding permits the auditor to decide which applications have audit significance, since an audit normally does not extend to all applications.

---

[9]Ibid., 29.

General Understanding of Extent EDP Used

The auditor must understand the flow of significant classes of transactions through processing activities in order to understand the extent to which computer processing is used. The information can be obtained by examining (a) the processing performed by EDP personnel and by computer programs and (b) the division of transaction processing flow between EDP and non-EDP activities. For each application, the study may include the following:[10]

1. Type and extent of documentation available for review.
2. Source document preparation or data capture procedures.
3. Data preparation or data entry procedures.
4. Files used or created.
5. Various output and reports produced.
6. Error correction procedures.

Basic Structure of Accounting Control for EDP

The investigation of the flow of transactions and the extent to which EDP is used in significant accounting applications provides the information about the basic structure of accounting control for EDP, which is complemented by a preliminary investigation of both general controls and application controls. General controls are

[10]Ibid., 30.

reviewed to provide an understanding of the client's computer data processing organization and the organizational assignments for three major areas of control: development, operations, and data and program files. The significant auditing applications are examined to gain a general understanding of the basic structure of the controls for each of the applications.

The application controls can be studied in terms of the flow of processing: (1) control over data recording and data preparation to ensure complete and correct preparation of authorized data; (2) input controls and input validation procedures to ensure complete input of valid data; (3) processing controls to ensure accuracy and completeness of output and distribution to authorized users; (4) output controls to ensure accuracy and completeness of output and distribution to authorized users; and (5) error handling for all the above steps and audit trail.

Preliminary Assessment

The review of the processing flow and the extent to which controls are applied are both general at this phase of the review. Documentation of the preliminary phase of the review may include completed questionnaires, simple narratives, simple flow diagrams, or notes identifying and briefly describing the controls in use. These document the auditors understanding of the data processing system, the

extent of EDP in each application having audit significance, and the preliminary understanding of general accounting controls and application controls. Documentation should include the planned effect of this assessment on the remaining portions of the audit.

The preliminary phase of the review provides sufficient information on the flow of processing and the structure of controls for the auditor to be able to make a preliminary judgement regarding further audit procedures. The auditor can decide to proceed with completion of the review. The decision may include reliance upon some controls, but not all controls. On the other hand, the auditor may decide not to proceed with completion of the review because internal accounting controls for EDP are inadequate or because the auditor knows that reliance will not be placed on internal accounting controls for EDP since, (a) alternative procedures for obtaining evidential matter are deemed more efficient or more effective or (b) other internal accounting control procedures outside EDP are in existence and deemed adequate.[11]

Completion of the Review

The completion of the review supplies the auditor a detailed understanding of the design of the general controls and the controls in the applications having audit

---

[11]Ibid., 31.

significance. The documentation of the completion of the review is more extensive than the documentation of the preliminary phase. It requires more detailed questionnaires and interviews, as well as more complete narratives, diagrams, and notes. In addition, it usually involves a system walk-through and the observation of the manual procedures and documents used in both the general and application control procedures.[12] Completion of the review of general controls includes the following:

1. Organizational and operational controls.
2. Application system development and maintenance controls.
3. Hardware and system software controls.
4. Access controls.
5. Procedural Controls.

Completion of the review of application controls includes additional in-depth investigation of the input, processing, and output procedures and controls in each application. The processing steps, audit trail, and control procedures should be documented for each application having audit significance and selected for review. The auditor reviews those controls on which he plans to rely.

After studying the results of the completion phase of

---

[12]Ibid., 31.

the review, the auditor can decide to rely on internal accounting control in computer data processing and proceed to compliance testing, based on the evaluation that controls as designed are adequate. The decision can include reliance on some but not all controls. The auditor also has the option not to rely on internal accounting control in computer data processing, in which case the auditor will not proceed with compliance tests.

Tests of Controls

Tests of compliance are designed "to provide reasonable assurance that accounting control procedures are being applied as prescribed. Test of compliance are necessary if the prescribed procedures are to be relied on in determining the nature, timing, or extent of substantive tests of particular classes of transactions or balances, but are not necessary if the procedures are not to be relied on for that purpose."[13] Tests of compliance are concerned primarily with certain questions. Were the necessary procedures performed? How were they performed? By whom were they performed?

The review defines the computer data processing system and the related controls as they are alleged to exist in the way setup by organization personnel and EDP documentation.

---

[13]AICPA, U.S. Auditing Standards, Vol. A (Chicago: Commerce Clearing House, Inc., 1988): 2165, Section 320.62.

If reliance is to be placed on these controls, the auditor needs to test the functioning of the controls.[14]

Test of compliance cover both general and application controls. The controls may be implemented by organizational design and visible procedures or by computer program logic. In the case of organizational design and visible procedures, tests of compliance use traditional techniques, such as the following:[15]

1. Observation.
2. Corroborative inquiry.
3. Inspection of documents containing evidence of compliance.

Control Structure

Where computer processing is used in significant accounting applications, internal accounting control procedures are sometimes defined by classifying control procedures into two types: general and application control procedures. Whether the control procedures are classified by the auditor into general and application controls, the objective of the system of internal accounting control remains the same; to provide reasonable, but not absolute, assurance that assets are safeguarded from unauthorized use or disposition and that financial records are reliable to

---

[14]Davis, Auditing & EDP, 30.

[15]Ibid., 31.

permit the preparation of financial statements.[16]

General controls are those controls that relate to all or many computerized accounting activities and often include control over the development, modification, and maintenance of computer programs and control over the use of and changes to data maintained on computer files. Application controls relate to individual computerized accounting applications, for example programmed edit controls for verifying customers' account numbers and credit limits.

[16]AICPA, "U.S. Auditing Standards," Professional Standards, (New York: AICPA, 1988) Section 320.34: 2156.

CHAPTER 3

GENERAL CONTROLS

The Auditor's Study and Evaluation of Internal Controls in EDP Systems classifies the general control features in most EDP-based accounting systems in five classifications as follow:

1. Organization and operation controls.
2. Systems development and documentation controls.
3. Hardware and systems software controls.
4. Access controls.
5. Data and procedural controls.

Organizational and Operating Controls

The effectiveness of many accounting control procedures depends on the activities of responsible personnel. For this reason, a well-planned and properly functioning organization is an important factor in accounting control. The organization plan forms a framework in which the operations function and which establishes the function relationships to each other. In an EDP system, the plan of organization should include these basic general controls:

1. Segregation of functions between the EDP department and users.
2. Provision for general authorization over the execution of transactions.
3. Segregation of functions within the EDP department.

Segregation of Functions Between EDP and Users

Segregation of functions should be maintained in computerized systems. The EDP department should be independent from the users and should control information to be processed. The EDP department should not correct errors unless they originate within EDP, for example, keypunch errors.

Review and test of compliance must be performed if the auditor plans to rely on this general control of segregation of functions between EDP and users. The auditor must make inquiries of appropriate personnel and review organization charts and job descriptions for evidence of proper segregation of functions. The auditor must note the degree of management supervision being exercised while observing the actual operations. The auditor must discuss with management and operating employees the extent and effectiveness of management supervision. The auditor would have to review management reports, studies, or evaluations concerning the operations of the data-processing system.

Authorization for Transactions

As a rule, the EDP department should not originate or authorize transactions, perform the initial data preparation for transactions, have custody of or control over non-EDP assets, be responsible for establishing controls, or have the authority to originate master file changes. In some cases an automatic journal entry or purchase order original transactions might be produced by the computer. Management should approve all transactions of significant dollar amount that the computer generates.

Some authorization process may be part of the computer programming. Whenever, possible an independently established control over transactions and master file changes, for example, item count, control total, and other authorization criteria should be established.

If the auditor plans to rely on these general controls the auditor must review and test for compliance. By reviewing the reconciliation of control totals maintained outside of EDP with the results of the computer processing. Examine evidence to indicate that the reconciliations that take place are in the normal course of operations. The auditor must review pre-processing, post-processing, or programmed controls to determine if they provide for processing in accordance with management's authorization.

Segregation of Functions

Segregation of functions should include the following: separation between operations and programming, an independent control group, implementation of a librarian function, rotation of operators, closed-shop operations, and required vacations for all employees. If the systems and programing departments are not independent of the operations department, the more likely the system will have an unauthorized modification to the programs or files.

Independent Librarian function may provide control in segregating the systems, programming, and operation departments by making data files and programs available only to authorized personnel for use in required processing. Additional controls may be provided in some systems through library-control software, either internally developed or purchased from an outside vendor. Also, rotation of operators usually reduces opportunities for undetected operator intervention during processing.

A closed-shop operation also contributes to the segregation of functions since programmers, systems analysts, and other non-operations personnel are not allowed to operate the computer nor be in the computer room when the program is being run.

If the auditor decides to rely on these general controls, one or more of the tests described below may be

performed:[17]

1. Observe EDP to determine that system analysts and programmers do not have unrestricted access to hardware, files, or programs
2. Review procedures for granting access to programs and data.
3. Observe control group to make sure independent with systems, programming, and operations group.
4. Observe librarian function, review logs and records to determine that usage records are correctly maintained and only properly supervised people are permitted to remove data files.

Organization and operations controls are so vital that major weaknesses could cause the auditor to have serious reservations about the reliability of results produced by the system. A programmer who operates the computer and has unlimited access to computer files might be in a position to commit and conceal a variety of irregularities. Strong controls in other areas may not completely compensate for this weakness. For these reasons, the auditor should consider the strength of organization and operation controls when reviewing other controls, particularly application controls.[18]

---

[17]AICPA, Internal Control of EDP Study, 30.

[18]Taylor, Auditing, 363.

Systems Development and Documentation Controls

These general controls relate to three areas: (a) review, testing, and approval of new systems, (b) control over program changes, and (c) documentation procedures.

System development and documentation controls should ensure that effective application controls are included in all new systems and should preserve the integrity of application controls after the system has been implemented. Management should approve application controls before they are implemented. When system development and documentation controls are properly designed, they can prevent or disclose the following types of errors:[19]

1. System implementation that do not have adequate application controls.
2. Systems that do not meet management objectives or operate to original specifications.
3. Implementation of systems that have not been properly tested.
4. Implementation of systems that are suspect to unauthorized modifications.

Procedures for System Design

The procedures for system design, including the acquisition of software packages, should require active participation by representatives of the users and, as appropriate, the accounting department and internal

---

[19]AICPA, Internal Control Study of EDP, 32.

auditors. The systems analyst and user department usually define systems requirements. Some difficulty can arise in communications between users in expressing their terms so EDP personnel can thoroughly understand.

Independent auditors are concerned with the existing system of accounting control. They will be interested in the relation of this control to new applications implemented during the period under review. The auditor will want to review applications prior to their implementation to help avoid future problems in accounting control and auditability.

If the auditor plans to rely on these controls he must undertake one or more of the following:[20]

1. Interview representatives of user departments for evidence of the level of their participation in systems definition.
2. Review documents and approvals to ensure user departments have an adequate understanding of inputs, processing requirements, control procedures, and system output.
3. Review the extent of the internal auditor's involvement in the definition of the systems and review their work papers.

Written Specifications

Each system should have written specifications which are reviewed and approved by an appropriate level of

---

[20]Ibid., 32.

management and applicable user departments.[21] Written specifications provides a bench mark for management in measuring the resulting systems. Approval by users and management contributes to the implementation of an adequately controlled system. Continuing review and approval of the system facilitates the monitoring and maintenance of an acceptable level of quality.

Review and test of compliance may be carried out by using either one or all of the following procedures:

1. Review the installation standards for systems design.
2. Review design specifications and look for written evidence of approval.
3. Interview management, users, and EDP personnel to determine what approval procedures are employed.

System Testing

System testing should be a joint effort of users and EDP personnel and should include both the manual and computerized phases of the system. This system testing will determine that a system operates in conformity with its designed specifications and that it satisfies the user's requirements. The testing should be designed to ensure that correct input will provide desired results and that it will provide detection of incorrect input, processing, or output.

This review or tests of compliance can be carried out

---

[21]Ibid., 32.

by the following:

1. Review testing standards, test data, and resulting output to determine if they appear to be reasonably comprehensive.
2. Interview user and EDP personnel to determine test procedures.
3. Perform processing using independently developed test data.

Final Approval

Final approval should be obtained prior to placing a new system into operations.[22] A system should receive final approval from appropriate levels of management before being used in normal operations. This includes examination of the final test results and review of documentation, changes from original design, and planned procedures for system implementation and operation.

To review and test compliance, review the evidence of the approval of significant accounting application systems. Also interview user and EDP personnel involved in the approval process, inquiring about their understanding of and satisfaction with the system.

Other Controls

One control is that all master file and transaction file conversion should be controlled to prevent unauthorized changes and to provide accurate and complete results. This

---

[22]Ibid., 33.

control will prevent errors from occurring in the conversion process. Appropriate personnel should establish control procedures, such as record counts, hash totals, and amount totals.

One control after a new system has been placed in operation, is that all program changes should be approved before implementation to determine whether they have been authorized, tested, and documented.[23] When a system has become operational, the integrity of the system should be maintained. There should be a formal procedure for requesting, authorizing, and approving all program changes. Personnel in charge of operating the computer should never be authorized to issue changes, but should verify changes that have been made before letting them be used in the system.

One last systems development and documentation control is that management should require various levels of documentation and establish formal procedures to define the system at appropriate levels of detail.[24] Management must establish formal procedures to create and maintain adequate documentation because there is a risk that EDP applications and systems may not be well documented. Documentation that is well done gives the auditor a better starting point for

---

[23]Ibid., 34.

[24]Ibid., 36.

review of accounting controls and helps facilitate program modifications and staff training.

Hardware and Systems Software Controls

The reliability of EDP hardware has increased dramatically over the last decade. This is primarily due to the chip technology. However, it is also due to the controls built into the hardware and systems software to provide for a self-diagnostic mechanism to detect and prevent equipment failures. Such controls are parity checks, echo checks, diagnostic routines, boundary protection and periodic maintenance.

Test of controls that cover hardware and system software controls test whether the controls are functioning as intended. In addition, audit software can be used to analyze the data collected by the diagnostic routines and detect significant trends.

Some types of failures will cause the device or system to halt. This type of control provides indication of a hardware malfunction. Failure to utilize available hardware controls could result in significant processing errors. Review procedures of the computer hardware should consist of the following:[25]

1. Hardware equipped with automatic detection features.

---

[25]Ibid., 37.

2. Periodic hardware maintenance is performed.

3. Formal procedures established to recover from hardware failures.

4. Authorization and control over implementation of, and changes to, operating systems software.

Systems software is important in that the integrity of a systems program, such as a compiler, should be maintained. There should be a formal procedure for requesting, authorizing, and approving all changes to systems programs.

If systems software does not function properly, the computer programs will not process data accurately. This inaccuracy in data processing could affect the degree of reliance that the auditor places on the system's processing and output.

Access Controls

Access controls provide safeguards to insure that EDP resources are properly utilized. Access controls are designed to help prevent or detect deliberate or accidental errors caused by (1) improper use or manipulation of data files, (2) unauthorized or incorrect use of a computer program, or (3) improper use of computer resources or a combination of these.[26] Access controls emphasize ways to prevent or detect improper or incorrect use of computer resources.

---

[26]Taylor, Auditing, 370.

There are a number of objective to implement the access controls here are some of them.[27] First, access to program documentation should be limited to those persons who require it in the performance of their duties. Unlimited access to program documentation could result in unauthorized changes to computer programs and data files. Placing specific people in charge of the documentation and maintaining logs of program and data use are some ways to prevent improper or incorrect program changes.

Second, access to data files and programs should be limited to those individuals authorized to process or maintain particular systems. Data files should be restricted to computer operators. Computer program documentation should be restricted to people authorized to make modifications to programs.

Finally, access to computer hardware should be limited to computer operators. Physical security devices can be used to partially implement this control. In addition, reviews of utilization reports and console logs can be made on a regular basis.

Access controls are a set of operating procedures designed to prevent unauthorized modifications to data files and programs or misuse of computer hardware. Weaknesses in these controls affect the integrity of the entire computer

---

[27]Ibid., 370.

system. Such weaknesses should be considered when reviewing related application controls.[28]

Data and Procedural Controls

Data and procedural controls provide a framework for controlling daily operations and establishing safeguards against processing errors. They are designed to ensure prompt and accurate processing of data. Although there are some duplication between data and procedural controls and other general controls, some procedures need to be discussed separately.[29]

1. A control or balancing function.
2. Written manuals in support of systems and procedures.
3. Capability to restore or replace lost, damaged, or incorrect files.
4. Internal auditors or some other independent group within the organization should review and evaluate proposed systems at critical stages of development.
5. Internal auditors or some other independent group within the organization should review and test computer processing activities.

A control function of some type should ensure that all authorized data are accurately processed. The function should follow up on errors detected during processing and ascertain that transactions with errors are corrected and

---

[28]Ibid., 370.

[29]Ibid., 371.

resubmitted by the proper party and verify the proper distribution of output.[30]

A written manual of systems and procedures for all computer operations should exist. This manual should provide management with specific or general authorization to process transactions. An example would be if management authorizes write-offs of customer accounts that are outstanding for more than 120 days, this policy should be in the systems and procedures manual so that computer personnel will follow this authorization in processing transactions.

Like other general controls, data and procedural controls are important to the auditor's reliance on computer processing. This processing, in turn, produces results used to prepare financial statements. Therefore, data and procedural controls relate directly to application controls and should be considered when reviewing them.

General controls must be in place for application controls to be effective. It would be of little benefit to the company to have computer programs that edit input data for accuracy, validity, and completeness if these same computer programs could be improperly altered by a variety of personnel. It would be of limited benefit to the company to have verification of input data if verification was performed by the same personnel who authorized the transactions.

---

[30]Ibid., 371.

CHAPTER 4

APPLICATION CONTROLS

During the review of application controls, the auditor would consider any weaknesses that exist within the general controls. The review might include only those controls and weaknesses related to significant accounting applications, rather than all EDP applications.

Application controls have been defined as follow:[31]

> Input controls are designed to provide reasonable assurance that data received for processing by EDP have been properly authorized, converted into machine sensible form and identified, and that data (including data transmitted over communication lines) have not been lost, suppressed, added, duplicated, or otherwise improperly changed. Input controls include controls that relate to rejection, correction, and resubmission of data that were initially incorrect.
>
> Processing controls are designed to provide reasonable assurance that electronic data processing has been performed as intended for the particular application; that all transactions are processed as authorized, that no authorized transactions are omitted, and that no unauthorized transactions are added.
>
> Output controls are designed to assure the accuracy of the processing result (such as account listings or displays, reports, magnetic files, invoices, or

---

[31]AICPA, Study of Internal Control of EDP System, citing AICPA, Statement on Auditing Standards No. 3, "The Effects of EDP on the Auditor's Study and Evaluation of Internal Control," (New York: AICPA, 1974), paragraphs 8a, 8b, and 8c.

disbursement checks) and to assure that only authorized personnel receive the output.

Input Controls

Input controls are designed to provide reasonable assurance that computer input is entered into the computer system accurately and completely. The following four types of input transactions need to be controlled.[32]

First, transactions entered into the system. Transactions of this type often represent the largest volume of activity, and, therefore, can generate the largest number of errors. Inventory purchases and merchandise sales are prime examples.

Transactions that update or maintain files. Examples are changes of credit status on accounts receivable master files and changes in inventory purchase prices on master files for pricing inventory. Failure to properly update files can have far-reaching effects on the reliability of the accounting records. In the first example, the effect could be an understated allowance for doubtful accounts because of sales made to poor credit risks. In the second example, the effect could be a materially misstated inventory account because of incorrect pricing of inventory items.

Thirdly, transactions that inquire into the status of

---

[32]Taylor, Auditing, 374.

records on computer files. An inquiry, in itself, does not change a file. An inquiry that produces an incorrect response about a record in a file could result in an incorrect decision concerning a transaction. If an inquiry into the credit status of a customer produces incorrect information, an incorrect decision to extend credit might be made.

Finally, transactions that correct errors made in previously entered transactions. An example is a transaction to change an expenditure from a fixed-asset addition to repairs expense. Correction of an error is often more complex than the original transaction and, if not handled properly, can create additional errors.

Individual Input Controls

Only properly authorized and approved input, prepared in accordance with management's general or specific authorization, should be accepted for processing by EDP.[33] If a transaction is supported by a document, some evidence of approval is needed. Time cards and purchase invoices are examples. If a transaction is entered without supporting document, a terminal user identification number or some other means of authorization should be used. The procedure of requiring authorization for transactions is conceptually no different in computerized than in manual processing. In

[33]AICPA, Study of Internal Control in EDP Systems, 51.

a computer system, however, unauthorized input may be harder to trace and correct.[34]

The system should verify all significant codes used to record data.[35] In many instances, computer processing is most efficient when codes are used to represent data. For example, a two-character numeric field could store codes that represent 99 geographic locations (36=New York, 24=Ohio, and so forth) whereas the use of names would require a much larger field. Codes are sometimes used to allow the system to perform functions more efficiently.

Conversion of data into machine-readable form should be controlled.[36] The use of control totals, hash totals, and record counts will help to detect errors made when data from source documents are transferred to magnetic tape, or some other device that can be read by a computer. When data are entered directly into a computer storage device through a terminal, a computer edit program will help to detect errors.[37]

Movement of data between one processing step and another, or between departments, should be controlled.[38]

---

[34]Taylor, Auditing, 375.

[35]AICPA, Study of Internal Control in EDP System, 53.

[36]Ibid., 53.

[37]Taylor, Auditing, 375.

[38]AICPA, Study of Internal Control in EDP Systems, 55.

When data are moved, they can be lost, added or altered. Control totals, hash totals, and record counts are also helpful in controlling correct movement of data.

Processing Controls

Processing controls are sometimes called programming controls. They consist of computer application programs that read the input data, test it for certain types of errors, and print out messages if such errors are found in the data. These computer programs also check for certain error conditions in files as updating runs are made.[39]

In general, processing controls are designed to prevent or detect the following types of errors:[40]

1. Incomplete or duplicate processing of input transactions.
2. Processing and updating of the wrong files.
3. Processing of illogical, incomplete, or unreasonable input.
4. Loss or distortion of data during processing.

Processing controls can also be used in manual processing by reviewing the source documents, journals, and other material that comprise the transaction trail. In a manual system these controls would have to be applied without the aid of the computer, which would be very

---

[39]Taylor, Auditing, 375.

[40]AICPA, Study of Internal Control in EDP Systems, 56.

tedious. Therefore, manual systems usually depend on other means to accomplish what the computer can accomplish in a computer system by checking detailed items of every input transaction.[41]

Individual Processing Controls

Control totals should be produced and reconciled with input control totals.[42] These totals should be produced at an early point in the application by originators of source documents or by a control group. They should not be forwarded to the computer department. The computer then produces its own set of control totals and an independent group then reconciles the two sets of totals.

Controls should prevent processing the wrong file, detect errors in file manipulation, and highlight operator-caused errors. Processing programs should check file identification, dates, or version numbers to determine that the proper file is being processed. External labels may be subjected to a manual check. For example, payroll check processing may be accurate in all respects, except for updating the wrong year-to-date earnings file.

Limit and reasonableness checks should be incorporated into the computer programs that edit the input data for

---

[41]Taylor, Auditing, 375.

[42]AICPA, Study of Internal Control in EDP Systems, 56.

errors.[43] The computer program checks the input data for illogical conditions that should not exist. Some examples are 200 hours on a weekly time card, inventory quantity reduced to a negative value, an unusually large check issued to a small-volume vendor, or acceptance of a credit sale for a closed account.

A wide variety of logical tests may be used to verify the contents and relationships of records during the processing cycle. Some of these tests include the following:[44]

1. Comparison data to a limit.
2. Test of data for illogical amounts in data fields.
3. Test for alphabetic data in a numeric field.
4. Test for zero value.
5. Validation of self-checking numbers.
6. Test of logical relationships between fields.

Output Controls

Output controls are designed to ensure that (1) the processing results are accurate and (2) only authorized personnel receive the output. A control group may be given the responsibility for implementing this control. They see that input data with errors are returned to the original

---

[43]Ibid., 58.

[44]Ibid., 58.

source, properly corrected, and resubmitted. A control group reconciles control totals generated by the computer with the same totals originated at an earlier point in the system. Finally, the control group sees that output reports are given to the appropriate personnel.[45]

Individual Output Controls

Output control totals should be reconciled with input and processing controls.[46] Reconciliations, such as balancing general ledger figures, should be performed by the user, control group, or a computer program used for processing.

Output should be scanned and tested by comparison to original source documents.[47] This control will prevent a master file with non-numeric data from having an error. Since this file cannot be controlled by balancing of totals. An inventory item might have an error in its description. The error could cause hundreds of shipments of a certain product to be in error.

Systems output should be distributed only to authorized users.[48] Output should be delivered on a timely basis to properly authorized users. In many instances the output is

---

[45]Taylor, Auditing, 376.

[46]AICPA, Study of Internal Control in EDP Systems, 60.

[47]Ibid., 60.

[48]Ibid., 61.

confidential such as payroll checks or inventory costs. An independent control group should be responsible for the distribution of all output.

CHAPTER 5

AUDITING TECHNIQUES USING EDP

The first decision an auditor must make is whether to audit around or through the computer. The auditor's objectives do not change when a client uses a computer for accounting applications. There are different audit techniques available to accomplish these objectives and the procedures may differ for several reasons.[49]

1. The nature of the audit evidence may change because certain information might be readable only by electronic or mechanical means.
2. Many of the client's internal accounting control procedures may differ from those applied in a manual environment.
3. The use of computer-assisted audit techniques may permit new audit tests that were not practical using manual testing.

The auditor's use of manual and EDP audit techniques should be integrated and complementary. As the auditor gains an understanding of the accounting system as a whole, the auditor can select from the possible audit techniques those most appropriate for the circumstances.

---

[49]AICPA, Computer-assisted Audit Techniques, (N.Y.: AICPA, 1979): 3.

Auditing through the computer gains importance as client EDP systems become more sophisticated. There are many techniques which auditors can use to audit through the computer to test EDP applications. Some of the more common techniques are described in the following sections.

Audit Software

The auditor may use various types of software on either microcomputers or main frame computers. For example, auditors often use microcomputer electronic spread sheets to prepare working trial balances, lead and other schedules. These spreadsheets significantly simplify the computational aspects of a task such as incorporating adjustments and reclassifications on a worksheet.

Three other types of software may be used on either a microcomputer or a main frame computer. They are generalized audit software, system utility software, and customized audit programs. Generalized audit software is used most frequently used because it allows the auditor to access various clients' computer files.

A generalized audit software package is a computer program or series of programs designed to perform certain data processing functions. Such functions include reading computer files, selecting desired information, performing calculations, and printing reports in a format specified by the auditor. Generalized audit software is useful to the

auditors for the following reasons.[50]

1. Auditors can learn to use generalized audit software effectively in a relatively short time without learning a programming language.

2. Allows examination of machine readable data--Generalized audit software allows direct access to data.

3. Facilitate documentation--Audit documentation is a by-product of the use this software.

Generalized audit software can be used to access client data maintained on computer files. Audit software can be used to access, reformat, and consolidate information that exists only temporarily and in machine-readable form and present it in a more meaningful and convenient manner.

Generalized audit software can deal with large quantities of data effectively. Audit software can scan, list exceptions based on the auditor's specified criteria, and summarize all data on a computer file. Thus routines such as footings, computations, and file-to-file comparisons, are more readily performed by the use of audit software.

Other uses are that generalized audit software reduces the reliance of the auditor on client EDP personnel. The software produces an efficient audit that can be used year after year with little or no modification. This software can further the auditor's understanding of the client's

---

[50]AICPA, Computer Audit Techniques, 4.

automated systems and operations.

Audit software is used to accomplish six basic types of audit tasks:[51]

1. Examine records based on criteria specified by the auditor.
2. Testing calculations and making computations.
3. Comparing data on separate files.
4. Selecting and printing audit samples.
5. Summarizing or resequencing data and performing analyses.
6. Comparing data obtained through other audit procedures with company records.

Test Data

To test programmed controls for compliance, the auditor obtains evidence that the controls are functioning properly. On technique, which involves the use of test data, was designed for batch systems. The method operates a follows.[52]

1. Client documentation is reviewed and controls are identified.
2. Simulated transactions, including records with errors, are created and entered in the system to test the identified controls.
3. These transactions are entered on the auditor's worksheet, along with the predetermined computer results.

---

[51]Ibid., 6.

[52]Taylor, Auditing, 417.

4. The simulated transactions are processed with the client's computer program, and the computer results are compared with the predetermined results. If the two sets match, the client's program is assumed to be functioning as called for in the program documentation.

When using test data, the auditor should obtain reasonable assurance that the program being tested is the one actually used for regular processing. A different program could be substituted for the regular one to satisfy the auditor and to appear proper. There is no assurance that this substitution will not occur, but precautionary steps can be taken to lower the probability of such an occurrence.

The test data could be run on a surprise basis. Another approach might be for auditors to copy the client's program in advance of the test data run. Later at the client's convenience, the test data could be processed, and the program used in this processing could be compared with the copy of the program obtained earlier.

A major benefit of using test data is the greater assurance that is gained about the reliability of the client's computer programs. However, the use of test data does have certain limitations.[53]

1. A successful test data run does not necessarily indicate a strong internal control structure. Other types of errors or irregularities could occur outside the computer processing area. An example

---

[53]Taylor, Auditing, 420.

is the failure of the mail clerk to report all cash receipts.

2. Test data determine whether the program that was furnished to the auditor is functioning as it should. The auditor cannot be certain that this is the same program that is used in daily operations, although proper precautions can greatly increase that assurance.

3. The test data approach was designed for a batch processing system. There is some question as to its suitability for the newer online systems where there is no intermediate processing between the input devices and the central processing unit, and where more continuous processing takes place.

4. Developing test data can be time-consuming and the test data must be tailor made for every application.

Even with these drawbacks, the use of test data is definitely a step in the direction of going through the computer and, with proper safeguards, can provide auditors with insights into the computer system that are not gained by ignoring the computer.

Integrated Test Facility (ITF)

This method introduces dummy transactions into a system in the midst of live transactions and is usually built into the system during the original design. Establishment of a "dummy" entity through which data can be processed; for example, a fictitious division, store, dealer, department, or any other basis of accumulation of accounting information.

After establishing the entity the auditor can process

transactions against the entity using the client's regular system. The ITF data is entered into the system with live data and processed in the same way as regular data. The auditor at some point should remove the test data from the system. The auditor determines the transactions or master file conditions to be tested and, as with any test data approach, compares the actual results of processing the ITF data to the predetermined processing results.[54]

The primary reason for the use of ITF is that the whole system can be tested, including the manual procedures as well as EDP. The auditor can monitor test data from the point of its authorization and input into the system, to its final disposition in output. The resulting transaction and file interactions caused by the test data can be reviewed, as can the manual procedures applied.

ITF may be more economical than other test data approaches. Since the auditor uses the company's normal documentation and input stream for entering transactions, the technique tends to be easier to explain to client management and therefore may be more readily accepted than some other computer audit techniques.

Parallel Simulation

The auditor develops a program to perform the same key functions as the application to be tested. The same data

---

[54]AICPA, Computer Audit Techniques, 47.

are processed using the client's application program and the auditor's simulation program. A theoretical advantage of this method over the traditional test data approach is the ability of auditors both to check the functioning of the client's program and to test the accuracy of the client's output.[55]

The results are compared. All discrepancies in the output of the two programs should be investigated. If the output is the same, or differences are satisfactorily explained, the auditor's understanding of the system is confirmed and there is some assurance that the client's program is processing data as intended. The auditor need not simulate all of the functions of a program, only the ones of audit interest in the circumstances.[56]

An advantage of the parallel simulation technique is that the auditor uses actual client data. Auditors can also run the client's program with actual data several times during the year. The purpose of this procedure is to provide relative assurance that the client's records have been processed consistently during the year.

Parallel simulation has several disadvantages. A complex simulation program can be time-consuming and costly to create, and the auditor needs a detailed understanding of

---

[55]Taylor, Auditing, 421.

[56]AICPA, Computer Audit Techniques, 76.

the client's application program. An auditor may choose to use generalized audit software to create the simulation program or take a specialized audit program approach.

This approach is a computer counterpart of the traditional test of transactions in a manual system, in which data are traced, for selected time periods, from source documents to journals and ledgers. In both procedures, auditors are attempting to satisfy themselves that record-keeping procedures are employed consistently. Undoubtedly, there are benefits to be gained from monitoring of this sort, but it could prove to be costly.[57]

Audit Work Station

More internal audit departments and a few external auditing firms are ending their dependence on audit software programs run on a mainframe by using an audit workstation. Using a microcomputer and the necessary software, the auditor extracts the necessary data from the client's files and performs the desired tests directly on the microcomputer.

---

[57]Taylor, Auditing, 421.

CHAPTER 6

UNIQUE CHARACTERISTICS OF SPECIFIC EDP SYSTEMS

Computer-based data processing may be performed in a number of ways. The processing method or approach affects the audit because it affects such factors as the complexity of the system, the internal accounting controls, the visibility of the audit trail, and the ease of record retrieval. These in turn affect the application of audit procedures and the availability of audit evidence.

The purpose of this chapter is to describe EDP systems that are commonly found in the business environment so the candidate will be able to apply the appropriate controls to the system in question. Computer data processing has traditionally identified two major methods of processing: online and batch. In on-line processing, individual transactions are processed immediately; in batch processing, batches of transactions are processed periodically.

Batch Processing

Batch processing is a common EDP system. There are three key points in a batch processing system. First, transactions flow through the system in batches and in any

particular batch, transactions may add, change, or delete information in the master file. Secondly, if CRTs are used in batch processing, it may appear to the user that batch file is set up and the transactions are processed later in the day. Known as an online system but not real-time. Thirdly, batch processing normally leaves a relatively easy to follow audit trail.

A batch processing system is sometimes called a method of periodic preparation and periodic processing.[58] This is because data from source documents are periodically transferred to magnetic tape. After the data on the tape are edited, a periodic computer processing is performed that creates an updated master file, as well as other output. If there is no need for frequent inquiry of a record, batch processing can be a feasible and relatively inexpensive method of entering and processing transactions for some applications.

Direct or Random Processing

Most newer systems employ direct access processing techniques known as online real-time (OLRT) because the response by the system to data input can arrive back to the user in time to affect the user's decision process and files are updated immediately. Such as an airline reservation system. Online processing does not require that data from

---

[58]Taylor, Auditing, 377.

source documents be transferred to machine-readable form before computer processing takes place. It is not even necessary that a source document be created when an online system is used although one may be created in the process. When a transaction occurs, such as a charge sale, the data are entered through a terminal into the permanent record, often maintained on magnetic disk. A record inquiry can be performed at anytime.

In direct processing transactions data is entered through online terminals and stored on direct access, disk storage. The edit routines immediately check the data for errors. Messages on the display prompt the user to correct and reenter the data. Master files and programs are stored online so that updating can take place as the edited data flows to the application. Output comes in the form of CRT displays and hardcopy reports produced periodically. Finally systems security must be in place to restrict access to programs and data to authorized persons only.

Data Base Processing

A data base is a set of interconnected files that users can access to obtain specific information. A data base eliminates the need for separate, and often repetitive, application-specific files.[59] For example, instead of payroll and personnel maintaining separate files that

---

[59]AICPA, Auditing & EDP, 141.

contain basically the same information and combines like files. Such storage of information may alter the audit trail.

Data base processing is dependent on an online real-time (OLRT) EDP system. CRTs can be used to directly access the data base. The common files, called data base, require strict control over access and changes to the data.

A company with database usually has a database administrator (DBA) function with one or more individuals responsible for database administration. The more complex the computer system and data structure, the greater the need for a central function to coordinate the sharing of data among users and to oversee the data base.[60]

Controls in this EDP system must start at the user department, with strict controls over who is authorized to read and/or change the data base. In addition to the usual controls over terminals and access to the system, data base processing also maintains controls within the data base itself. These controls limit the user to reading or updating only authorized sections of the data base. Because the data base is being updated on a continuous basis during the day, a backup of the data base should be made at the end of each day.

---

[60]AICPA, Auditing & EDP, 109.

Small Computer Environments

In the late 1970s, small, low-cost computer systems began to be used for business data processing applications. In recent years computer technology has produced a number of systems that can be used by both large and small businesses. Special audit problems are created with these systems. In this section minicomputers and microcomputers will be discussed with some of the control problems and ways to address them.

Minicomputer

A minicomputer is a small computer system, but generally one with more capabilities than a microcomputer. The minicomputers are essentially down-sized large computers with powerful processing capabilities but with limited input and output devices. For example a company may have a minicomputer to handle its accounts receivable or payroll function. These types of computers are often operated by a small staff of personnel that are computer users rather than professionals. Minicomputer systems often lack the physical security of larger computer systems. In addition, minicomputer systems make considerable use of online entry and online updating.[61]

The controls that auditors should evaluate depend on the system in use. Some systems operate from a central

---

[61]Taylor, Auditing, 380.

computer and store data in a central location. Each minicomputer in the system updates the central data base, as well as maintains files in its own areas. This gives minicomputers some of the same characteristics as online systems with terminals a various locations.

Other systems have their own independent equipment and files. Files are updated when processing takes place; there is no updating of a central data base. Audit trails must be created on printed output rather than through magnetic media. To provide an adequate audit trail for logging transactions, it might be necessary to add a magnetic tape or disk storage device to the system.

If a system has independent equipment and files, each minicomputer location may have its own set of controls. Given these characteristics, these systems have special control problems that may not exist in larger installations. Some potential problems are:[62]

1. Lack of segregation of duties among programming, operations, and control of data within the computer department.
2. Inadequate processing controls in programs furnished by vendors, especially controls applicable to online processing.
3. Access to data files and programs by a number of individuals.
4. Lack of control over program changes, caused by the fact that the same person who makes program changes in a minicomputer installation often controls data

---

[62]Ibid., 381.

files and enters transactions.

If there is a segregation of functions between the user department and the computer department, the user department should do the following:[63]

1. Authorize transactions.
2. Use batching or other appropriate procedures to determine that all input is processed.
3. Have control over changes to master files and resubmission of transactions rejected by computer edit programs.
4. Balance master files from one processing cycle to another.

If the minicomputer system uses online updating, there should be limited access to the terminals and use of passwords. It is also advisable for user departments to keep transaction and master file totals and to periodically balance these totals with those generated by the computer system.

Microcomputer

Microcomputer refers to a very small personal computer system. Microcomputers perform a variety of functions on a stand alone basis. Microcomputers clearly need internal controls, but too much control may stifle the unique

---

[63]Ibid., 382.

microcomputer operating environment.[64]

Control procedures should attempt to insure data and system integrity without suffocating the system. The most important controls in an automated system are accounting controls. Accounting controls operate to safeguard assets and to insure the reliability of data.[65]

Some control problems of microcomputers are that there is no separate computer staff. Microcomputer users are trained to perform certain applications. Microcomputers are not in a controlled area in a computer center. Among other things, this causes a problem of physical security. Also files are often stored on removable floppy diskettes.[66]

To address these shortcomings management should insure adequate training of personnel who will use the microcomputers. Document the duties of the personnel. Label diskettes and keep in separate secure storage. Make a backup copy of all files. Protect the software stored in the microcomputer and frequently printout data processed by the computer. With the expanded use of microcomputers it may be necessary to devise new control procedures for these systems.

---

[64]Wolfe, Christopher and Casper E. Wiggins, "Internal Control in the Microcomputer Environment," Internal Auditor, 43 (December 1986): 57.

[65]Ibid., 58.

[66]Taylor, Auditing, 383.

CHAPTER VII

CONCLUSION & SUMMARY

EDP technology has brought to the business environment many changes. Since the early 1970s the explosion of the computer technology and use by businesses has created internal control concerns for auditors, managers, and accountants. These groups must adapt to the changing technologies if they are to have control of the accounting records.

EDP departments must work closely with user departments in the development of new application systems. When system development teams develop new application software they must be aware of the internal control procedures and seek information from the audit department to assure that these controls are included to provide adequate safeguards. Management will have to be conscious of the control environment in which they operate. Different review techniques may be required in the future to ensure the accuracy of data output from EDP systems. As new EDP systems are developed controls relating to access and updating of information within the system will have to be considered.

Managers, accountants, and auditors must enhance their computer skills if they are going to continue to function in the modern world of business computers. The business environment has become very complex with all the new technologies and advancements in the computer industry. If managers, auditors, and accountants ignore this expansion of EDP technology and knowledge it will make them obsolete and will jeopardize the security and integrity of company data.

For a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies they must have an internal control structure that will enable them to achieve such a goal. The only way to achieve this goal is for the company to determine the degree of control they desire and set up an internal control structure to meet those needs.

SELECTED BIBLIOGRAPHY

American Institute of Certified Public Accountants, Computer Services Executive Committee, The Auditor's Study and Evaluation of Internal Control in EDP Systems, (New York: American Institute of Certified Public Accountants, 1977).

American Institute of Certified Public Accountants, Computer Services Executive Committee, Computer-assisted Audit Techniques, (New York: American Institute of Certified Public Accountants, 1979).

American Institute of Certified Public Accountants Professional Standards, U.S. Auditing Standards, (Chicago, Illinois, Commerce Clearing House, Inc., June 1, 1988.)

Bailey, Andrew D., "Ticom and the Analysis of Internal Controls," Accounting Review, 60 (April 1985): 186-201.

Brink, Victor Z. and Herbert Witt, Modern Internal Auditing: Appraising Operations and Controls, New York, N.Y., John Wiley & Sons, Inc., 1982.

Carmichael, D. R., "Audit Procedures in a Data Processing Environment," CPA Journal, 56 (August 1986): 82.

Cummings, William, Joachim Lauer and Richard Baker, "Expert Systems in Internal Auditing," Internal Auditing 58 (Summer 1988): 49-64.

Davis, Gordon B., Donald L. Adams and Carol A. Schaller, Auditing & EDP, (New York, N.Y.: American Institute of Certified Public Accountants, 1977).

Doost, Roger K., "Small Business Audit of a Computerized Entity: A Different Challenge for the Auditor," CPA Journal, 58 (September 1988): 96-99.

Dunmore, David B., "Using Audit Master Plan," Journal of Accounting and EDP, 3 (Winter 1988): 30-4.

EDP Auditors Foundation, "General Standards for Information Systems Auditing," EDP Auditors Journal, 1 (1988): 65-72.

Esposito, Ralph W., "Audit Effects of Computer Processing," CPA Journal, 55 (January 1985): 67-68.

Fields, Kent T., "Assignment of Audit Responsibility in Computer System Development Projects," Journal of Information Systems, 2 (Spring 1988): 51-57.

Gerlach, James H., "Model for Testing the Reliability of Computer Programs and EDP Management: Internal Control Implications," Auditing, 7 (Spring 1988): 61-76.

Kirby-Paz, Barbara, "Challenge of Auditing Computerized Systems," Internal Auditing, 3 (Winter 1988): 72-76.

Klimowsky, Bruce M., "SAS No. 48--Effects of Computer Processing on Examination of Financial Statements." CPA Journal, 55 (February 1985): 69-70.

Lawler, Stephen J., "Review of EDP Technology and Its Effects on Internal Control." Controller Quarterly, 3 (1987): 25-28.

Mohrweis, Lawrence C., "Usage of Concurrent EDP Audit Tools," EDP Auditor Journal, 3 (1988): 49-54.

Munter, Paul and Thomas A. Ratcliffe, "Impact of Computer Processing on Financial Audits," CPA Journal, 55 (January 1985): 34-6, 38.

Stewart, Trevor R. and Randy Finch, "Developing a Microcomputer Program for Evaluating Internal Control," Internal Auditing, 2 (Summer 1986): 31-9.

Reilly, Robert F., "Internal Audit considerations of SAS No. 48," Internal Auditing, 1 (Spring 1986): 42-6.

Sourwine, Darrel A., "How Are Your Internal Controls?" Internal Auditor, 44 (June 1987): 41-44.

Taylor, Donald H. and G. William Glezen, Auditing: Integrated Concepts and Procedures, New York, N.Y., John Wiley & Sons, 1988.

Wallace, Wanda A., Hand Book of Internal Accounting Controls, Englewood Cliffs, N.J., Prentice-Hall Inc., 1984.

Watson, Robert D., "Use of Microcomputers in the Audit Environment," EDP Auditor Journal, 1 (1988): 31-42.

Wiggins, Casper and Christopher Wolfe, "Microcomputers in Auditing; A Primer," Journal of Accounting and EDP, 4 (Spring 1988): 47-50.

Wolfe, Christopher and Casper E. Wiggins, "Internal Control in the Microcomputer Environment," Internal Auditor, 43 (December 1986): 54-60.

Wu, Frederick H. and Ronald A Safran, "A Practical Approach for Evaluating EDP Controls," CPA Journal, 57 (October 1987): 58,60-2,64-6,68-9.