5-1981

Auditing in an Electronic Data Processing Environment

Terry L. Moore

Auditing in an Electronic Data Processing Environment

by

Terry L. Moore

An Independent Study
Submitted to the Faculty
of the
University of North Dakota
in Partial Fulfillment of the Requirements
for the Degree of
Master of Accountancy

Grand Forks, North Dakota
May
1981

TABLE OF CONTENTS

CHAPTER 1

The development of computer based information systems is taking place at a rapid pace. Data processing technology linked with communications technology results in sophisticated information systems available to many users, large and small. In the future, most of the activities within a business enterprise will interact in some way with a computerized system. As the computer's importance to the business enterprise increases, the significance of control and management over a computer based system becomes greater.

The purpose of this paper is to establish a better understanding of the effects that computer technology is having on the auditing profession. The reason is that auditors are becoming more and more affected by the existence of computers within accounting information systems. Therefore, an adequate knowledge of auditing Electronic Data Processing (EDP) is needed.

An adequate knowledge of electronic data processing systems is needed to conform to generally accepted auditing standards. The first standard in Statement on Auditing Standards (SAS)-1, Paragraph 210 deals with training and proficiency.

".01 The first general standard is: The examination is to be performed by a person or persons having adequate technical training and proficiency as an auditor."[1]

---

[1]Statement on Auditing Standards (SAS) No. 1. "Codification of Auditing Standards and Procedures," AICPA (New York: 1979), Section 210.01.

If an auditor was to be lacking in "adequate technical training and proficiency as an auditor", how could he objectively express an opinion on the fairness of the financial statements?

Also another general standard comes into play concerning the auditors need for computer knowledge. The third standard in SAS-1, paragraph 230 deals with "due professional care".

".01 The third general standard is: Due professional care is to be exercised in the performance of the examination and the preparation of the report."[2]

.03 A paragraph appearing in Cooley on Torts often cited by attorneys in discussing due care mertis quotation here:

> Every man who offers his service to another and is employed assumes the duty to exercise in the employment such skill as he possesses with reasonable care and diligence. In all these employments where peculiar skill is prerequisite, if one offers his service, he is understood as holding himself out to the public as possessing the degree of skill commonly possessed by others in the same employment . . ..[3]

If an auditor was to be lacking in skills commonly possessed by the profession, how could he objectively express an opinion on the fairness of the financial statements?

Therefore, this paper will discuss why the auditing profession needs an adequate knowledge of computers. To accomplish this objective, this paper will be divided into five chapters.

The first chapter will be the introduction to the paper, containing an argument for the need of the computer education in the auditing profession.

---

[2]Ibid, Section 230.01.

[3]Ibid.

The second chapter will discuss the auditing function and why the understanding of the information system is so important. Next a discussion on information will follow disclosing desirable characteristics that information should contain and why computers help to obtain these characteristics. Then a discussion will be presented reinforcing the need for computer education.

The third chapter will emphasize the potential dangers of computer abuses when using computers as a primary source of data processing. In so doing, a discussion of selected past cases of computer abuse will be presented. After discussing those cases of computer abuse, a classification scheme will be presented. Then some comments on possible computer abuses still to be detected will be presented.

The fourth chapter will discuss some auditing implications caused by the utilization of the computer and some techniques available to the auditing profession while involved in an audit engagement.

Then a fifth chapter will be presented as a summarization of the paper. In this summarization a discussion will be presented reinforcing the topics expressed throughout this study.

CHAPTER II

The objective of this chapter is to emphasize the overall importance the computer has made on the information systems and why it has affected the audit function.

First of all this chapter will define auditing and the objectives associated with auditing. Second this chapter will define an organization and why information is so important to an organization. Next this chapter will try to reason out why the information system is so important in the examination of the financial statements. Then a discussion will follow on the characteristics of information and why computers help to facilitate the information process.

According the Funk and Wagnall's New Standard Dictionary of The English Language an audit is "1) An official examination of accounts, and their verification by reference to vouchers, etc., 2) A calling to account".

However, to a Certified Public Accountant (CPA) auditing is much more than just a verification or examination of accounts. Auditing involves an examination of the organization. The reason is that in one way or another each segment of the business affects the financial status of the organization. As stated in the AICPA's Professional Standard, "the objective of the ordinary examination of financial statement by the independent auditor is the expression of an opinion on the fairness with which they present financial

position.. . ."[4] In order to express such an opinion, the auditor must look at the whole organization.

Referring back to Funk and Wagnall's New Standard Dictionary of the English Language an organization is "the systematic union of individuals in a body whose officers, agents, and members work together for a common end." To facilitate the working together for a common end, an organization has to have useful and effective information.

Then what is information? Information is generally considered to designate data arranged in ordered and useful form.[5] Thus, information is usually thought of as relevant knowledge, produced as output of processing operations, and acquired to provide insight in order to (1) achieve specific purposes, or (2) enhance understanding.[6] From this definition, information is the result of a transformation process, just as raw materials are transformed into finished products by a manufacturing process.

Therefore, if a CPA is to express an opinion on the financial statements of an organization, the CPA must be familiar with the system providing the information. The reason is that information is the backbone that holds the organization together and if the CPA is knowledgeable enough about the backbone of the organization, he can be in a better position to express an opinion.

Information is needed in virtually every field of human thought

---

[4] Ibid, Section 110.01

[5] Sanders, Donald H. Computers in Business. 4th Ed., (New York: McGraw-Hill, 1979), p. 7.

[6] Ibid.

and action. At a personal level, if you always had high-quality information you could take better advantage of your future career opportunities and you would be better equipped to make other personal decisions.

But besides being essential to individuals who use it to achieve personal ends, information is also needed by managers in organizations. Managers at all levels must perform such basic management tasks or functions as planning, organizing, staffing and controlling. The success of any business is determined by how well its executives perform these activities. How well these functions are carried out is, in turn, dependent, in part, upon how well the information needs of managers are being met. Why is this? It is because each function involves decision making, and decision making must be supported by quality information. If a manager's information is of poor quality, the decisions that are made will probably suffer and the business, at best, will not achieve the success it might have had.

In summary, quality information in the hands of those who can effectively use it will support good decisions; good decisions will lead to effective performance of managerial activities; and effective managerial performance will lead to successful attainment of organizational goals. Thus, information is the bonding agent that holds an organization together.

As a general rule, the more information serves to reduce the element of uncertainty in decision making, the greater its value. But information is one of the basic resources available to managers,

and like other resources it is usually not free. It is therefore necessary that the cost of acquiring the resource be compared with the value to be obtained from its availability. In other words, information should be prepared if: 1) its cost is less than the additional tangible revenues produced by its use, 2) it serves to reduce tangible expenses by a more than proportionate share or 3) it provides such intangible benefits as greater insight, faster reaction time, better customer service, etc., which the information user considers to be worth the costs involved.[7]

Along with the above economic considerations there are some other desirable characteristics that information should possess; accuracy, timeliness, completeness, conciseness, and relevancy.[8] Up to a certain point, information that possesses these properties may be expected to be more valuable than information lacking one or more of these characteristics.

Accuracy

Accuracy may be defined as the ratio of correct information to the total amount of information produced over a period of time. If, for example, 1000 items of information are produced and 950 of these items give a correct report of the actual situation, then the level of accuracy is 95%. Whether or not this level is high enough depends upon the information being produced. Fifty incorrect bank balances in a mailing of 1000 bank statements would hardly be acceptable to depositors or to the bank. On the other hand, if physical inventory

---

[7] Ibid., p. 14.

[8] Ibid.

records kept on large quantities of inexpensive parts achieve an accuracy level of 95%, for example, in the case of the parts inventory, greater accuracy could be obtained, but the additional value to managers of having more accurate inventory information might be less than the additional costs required. Inaccuracies are the result of human errors and/or machine malfunctions. Human error (in system decision, machine operation, the preparation of intput data, and other ways) is the primary cause of inaccuracy.[9]

Timeliness

Timeliness is another important characteristics. It is of little consolation to a manager to know that information that arrived too late to be of use was accurate. Accuracy alone is not enough. In the case of regular reports, an immediate response time following each transaction would involve a steady outpouring of documents. The result might well be a costly avalanche of paper that would bury managers. Thus, a compromise is often required. The response time should be short enough so that the information does not lose its freshness and value, but it should be long enough to reduce volume (and costs) and reveal important trends that signal the need for action.[10] The most appropriate information interval is therefore a matter which must be determined by each organization.

Completeness

Most managers faced with a decision to make have been frustrated at some point in time by having supporting information that is accurate,

---

[9] Ibid.

[10] Ibid., p. 15.

timely, but incomplete. An example of the consequences of failure to consolidate related pieces of information occurred at Pearl Harbor in 1941. Historians tell us that data available, in bits and pieces and at scattered points, if integrated, would have signaled the danger of a Japanese attack.[11] Better integration of the facts available at scattered points in a business for the purpose of furnishing managers with more complete information is a goal of information systems designers.

Conciseness

Many information systems have been designed on the assumption that lack of completeness is the most critical problem facing managers. This assumption had led designers to employ an ineffective approach, peppering managers with more information than they can possibly use. Important information, along with relatively useless data, is often buried in stacks of detailed reports. Managers are then faced with the problem of extracting those items of information that they need. Concise information that summarizes the relevant data and that points out areas of exception to normal or planned activities is what is often needed by, but less often supplied to, today's managers.[12]

Relevancy

Relevant information is "need-to-know" information that leads to action or provides new knowledge and understanding. Reports that were once valuable but that are no longer relevant should be discontinued.

---

[11] Ibid.

[12] Ibid.

As long as an important resource is supplied when and where it is needed, in the right quantity and quality, and at a reasonable cost, the resource tends to be taken for granted. It is often only when the supply, quality, and/or cost of the resource deteriorates that its importance is recognized. So it is with management information. Several weaknesses have been encountered with earlier information systems that have often prevented users from receiving information that possessed the desirable properties discussed above. And as pressures to improve the quality of management information have built, managers have often turned to computer usage for relief.

Included among the weaknesses that have contributed to information improvement efforts are:[13]

1) Difficulties in handling increased workloads. Processing capability in many firms has been strained by a) the growth in size, complexity, and multinational scope of the firm; b) the increased requirements for data from external sources such as local, state, and federal government agencies; and c) the demands of managers for more kinds of information. Fortunately, the greater the volume of data that must be processed, the more economical computer processing becomes relative to other processing methods.

2) Failures to supply accurate information. If a processing system has gone beyond the capacity for which it was originally planned, inaccuracies will begin to appear and the control of organizational activities will suffer. Computer processing, however, will provide more accurate information, if the tasks to be performed

---

[13] Ibid., p. 16.

have been properly prepared.

3) Failures to supply timely information. Meaningful information is timely information, but with an increase in volume, there is often a reduction in the speed of processing. Managers demand timely information. Unfortunately, although they may receive information about areas of virtual certainty in short order, information that reduces the element of uncertainty is often delayed until such time as it is merely collaborative. Thus, many businesses have turned to the use of computers to speed up their processing.

4) Increases in costs. The increasing labor and material costs associated with a noncomputer processing operation have often caused managers to look to computer usage for economical relief. For example, when compared with other alternatives, the use of computers may make it possible for certain costs to be reduced while the level of processing activity remains stable.

As mentioned above, good information should possess the desired properties and characteristics that managers need in making effective managerial decisions. In order for information to possess such a wide variety of characteristics such as accuracy, timeliness, completeness, conciseness, and relevancy, improvements in information systems were required. Thus technological research led to the development of the computer.

No where has the computer had a greater impact than on business. Just within the past 20 years, it has made business more of a science and has overturned long-established modes of managing organizations.[14]

---

[14]Carroll, Archie B., and Watson, Hugh J., Computers For Business (Dallas: Business Publications, 1976), p.3.

Some experts estimate that nearly half of all computers in existence today are used for business applications.[15] Only a few examples can demonstrate the profound influence computers have had on business and the managing of organization: automated payroll accounting, inventory control systems, fully computerized industrial plants, automatic customer billing, sophisticated computer forecasting, and comprehensive management information systems.

The Computer: A Brief Description

A computer is a high-speed machine which receives data and instructions, processes the data into information, and then furnishes the results in a form which is readable either by a person or another machine.[16]

The major advantages of the computer as a data processing instrument are its speed, its accuracy, and its capacity for storing vast amounts of data. The speed of the modern computer is almost too great to comprehend. It can add two 20 digit numbers in only a few millionths of a second, and it has printers that can generate output at the rate of 1000 or more lines per minute. In fact, the computer is so fast that in seconds it can perform work that would ordinarly take several men many years.

The computer's capacity for handling extremely large quantities of work, and its capacity for storage and high-speed retrieval, make it indispensable for most modern businesses. Computers are especially productive in handling jobs which are repetitive, tedious,

---

[15] Ibid.

[16] Ibid., p. 4.

and time consuming. In addition, with their ability to store large masses of data and to retrieve needed data quickly, computers provide a means for coping with the increasing complexity of business.

The disadvantages of the computer are somewhat misleading. It is usually not the disadvantage of the computer that are at issue but rather faults emanating from the people associated with it. For example, most customer billing errors are not due to the computer's computational errors but result either from data inputs that were incorrectly specified or difficiencies in the computer's operating instructions--and both of these are human mistakes.[17] Yet it is not uncommon to hear the charge that the computer made a mistake. For most people it is much more convenient to blame a machine which lacks human feelings than it is to single out the true source.

However, the computer is a vehicle for many of the horror stories that are popularized by the media. Computer costs can go out of sight with few tangible returns, some computer systems never live up to their vendor's presale claims, the computers output is not always appropriate for management's needs, the data stored in large computer systems can be grossly misused.[18] But these are unfavorable developments that can be eliminated or minimized by effective managerial action.

The primary reason computers have experienced such tremendous

---

[17] Ibid.

[18] Ibid., p. 5.

growth can be summed up in one word--applications. If it were not possible to make so many applications in the business world, computers would hardly have gained such widespread acceptance. And, if these applications did not prove to be economically justifiable and feasible, continued development would have been curtailed. Managers are pragmatic people, and this characteristic has led them to initiate an apparently unbounded growth cycle for computers. New applications of the computer are being discovered at such a rapid pace that it would be impossible for all but the most sophisticated information system to monitor and catalog the progress.

Business Applications of the Computer

There are a number of reasons why computerized data processing has become necessary and attractive to many business organizations. Perhaps the most fundamental one is related to the sheer size or volume of paperwork to be processed. As business organizations experience rapid rates of growth, there are noncommitant increases in the number of personnel needed to handle the resultant paperwork. Thus the volume of paperwork which must be processed, and the related increasing numbers of personnel needed to perform this work, drive costs to the point where managers have an attractive incentive for developing less costly ways of handling these tasks.

Computers, with their large storage capacities, make it possible to store vast quantities of organizational data. This data can be accessed with a speed that far exceeds that of manual systems. Most large business firms could not effectively compete without systems for the speedy retrieval of data.

Another major advantage of computerized data processing is

accuracy. After computer applications have been carefully developed and tested, few errors of computer origin ever occur. Most "computer mistakes" can be traced back to human origins.

When computers first appeared on the business scene, they were used primarily for routine data processing applications such as record-keeping and payroll preparation. In other words, the computer assumed the elementary role of performing clerical operations. More extensive applications evolved as technology improved and managers and computer specialists learned more of what could be done with the computer.

Part of the larger sphere of application can be attributed to an increase in the sophistication and usefulness of management science techniques (quantitative approaches to solving management problems). The developments in the management sciences came about because of the need to make decision making a more rational, information-using process. Many management science techniques require the availability of a computer, and it is not surprising that computers and the management sciences have matured hand in hand.

There are several areas in which the computer has proven to be extremely useful in the accounting function. These pertain primarily to routine applications such as sales accounting, payroll preparation, accounts receivable, and customer billing. In general, these are bookkeeping or recordkeeping functions that involve considerable amounts of data but only simple arithmetic calculations. In each of these areas, the computer provides the advantages of speed, storage capacity, and accuracy, along with decreased clerical expenses.[19]

---

[19]Ibid., p. 29.

Computer applications in accounting and finance, however, have become increasingly sophisticated in recent years. For example, computers are being employed to simulate an organization's future financial status. This type of simulation involves the construction of a mathematical model of the firm's financial picture (e.g., revenue, costs, cash flow, income), which is then manipulated in order to analyze possible outcomes under varying sets of conditions. Information of this type is useful to support decision making.

In addition to simulation, the importance of the computer in the finance and accounting function has been enhanced by its provision of reports which aid management in its performance of its planning and controlling functions. The capabilities of the computer make it easier for management to have access data and reports which during precomputer days could not be economically and/or accurately assembled. In fact, the ease with which the computer can generate reports has the potential for creating a paperwork jungle which, if left uncontrolled, could swamp managers with data and information. Consequently, control mechanisms must be developed to aid management to determine the need and justification for existing and projected reports.

Potential Problems

The accounting and finance areas have been made more sophisticated by the availabilities of the computer, but these advancements have not been made without problems. For example, complex computer accounting systems raise serious questions about possible fraud. In recent years, numerous cases of fraud, theft,

and embezzlement have been associated with EDP systems.

The most notable case of computer assisted fraud occurred in the 1973 Equity Funding Life Insurance scandal, in which the computer aided a large number of equity funding employees in a $60 million fraud scheme. Though most data processing professionals at the time scoffed at the idea of a "criminal computer", the computer field in general was indicted for not having appropriate controls and safeguards to insure against such occurrence. What makes this case especially intriguing, however, is the fact that Equity Funding's vice president for management information systems insisted that the equity data processing division had the same basic controls as 90 percent of the computer installation in the country.

It thus appears that present safeguards and control mechanisms that are built into accounting systems do not control 100 percent against abuses. The audit function in accounting has therefore necessarily taken on a new dimension, checking for computer-assisted theft.[20] Hence, with the many benefits of the computer have come potential problems which must be dealt with by management.

However, management is not the only party involved in dealing with those problems. The CPA must also learn to effectively deal with the introduction of the computer. It was recognized by the accounting profession in the mid 1960's, in a book called Horizons for a Profession.[21]

---

[20] Ibid., p. 31.

[21] Roy, Robert H., and MacNeil, James H., Horizons For a Profession; The Common Body of Knowledge for Certified Public Accountants. (New York: AICPA, 1967).

In 1967, Horizons for a Profession was published and accepted by the AICPA as an official pronouncement which emphasized in part, the impact the computer had made and will make on the accounting profession.

In this connection, important introductory points made therein are clear and unambiguous:

> Tomorrow's CPA will not be able to avoid the computer in his professional practice.
>
> CPA's who concentrate their practices in auditing and even those who engage only infrequently in this traditional area will encounter computers in the information systems of their clients organizations and, when they do, will discover that the audit trail has acquired new dimensions and characters.
>
> Whether the CPA's role is made more or less difficult by the presence of computer is secondary, the important thing is that the audit trail now is a different kind of labyrinth. Now the CPA must know when it is sufficient to scrutinize the flow diagram and the computer program, when and what kind of test data must be processed through the machine to verify its accuracy and scope, when machine input must be examined for accuracy, completeness and integrity, when dual processes are needed for adequate control, when and what stored data must be printed out for audit scruity, when the program itself must be modified to provide checks needed for internal control.
>
> More specifically, the CPA must realize that he cannot expect computerized systems to be modified to provide output that only he needs in order that he may perform his audit in the traditional way. Not only can this be too slow and costly, but it encourages the auditor to perform as though the computer were not there. Wherever practical, the CPA should audit through the computer; he must modify his emphasis so that he is concerned not only with the output, but with the system which produces that output.
>
> All of this does not mean that CPA's will not continue to verify results. It means only that their verification procedures must change in parallel with the changes in methods of producing results.
>
> CPAs have been engaged in auditing for a long time,

> now they must learn how to carry out the hallmark service of their profession in new ways.[22]

Conclusions

The purpose of this chapter was to emphasize the overall importance the computer has placed on the business world and why it has affected the audit function.

In order to accomplish that objective, this chapter discussed many things. First of all this chapter defined auditing and the objectives associated with auditing. Second this chapter defined an organization and why information is so important to an organization. Third, a discussion was presented trying to reason out why the information system is so important in the examination of the financial statements. Then a discussion was presented on the characteristics of information and why computers help to facilitate the information process.

---

[22] Horizons For a Profession, (New York: AICPA, 1967), Quoted in (or "Cited By") Arnold Schneidman, "Need for Auditors Computer Education." CPA Journal 49 (June 1979): 29,30.

CHAPTER III

The purpose of this chapter is to emphasize the potential weaknesses that are inherent in a computer based information system. In order to accomplish this objective, this chapter will present a few cases of computer abuse, covering one case in detail and the other cases in general. Next, this chapter will group cases of computer abuse into six major categories according to a study conducted by Donn B. Parker of the Stanford Research Institute. Then this chapter will discuss the possible computer abuses that are still to be detected.

Equity Funding

In 1973 a case that surprised many involved Equity Funding Life Insurance, in which the computer aided a larger number of Equity Funding employees in a $60 million fraud scheme. What makes this case especially interesting, it that Equity Funding's Vice President for management information systems insisted that the Equity Data Processing Division had the same basis controls as 90 percent of the computer installations in the country.

What Happened to the Files?

> What most likely happened at Equity was that an actuary or other dp (Data Processing) user was allowed access to the live master file of insurance policies to use as test data with a "model office" program to simulate the operation of the Equity Funding Life Insurance Co. in coming years. He used existing records to generate volumes of "test" data that somehow became

"real" input to later master file updates.[23]

The major difference between the old legitimate records and the newly manufactured records was that a special department number was assigned (in this case department "99") that caused the records to be skipped over when it came to the billing cycle.

In most cases the fake records did not have to be supported by real paperwork. If an auditor ever asked to see the policy application, medical history, or other papers, he was put off long enough for someone within the company to generate some for him. Ronald Secrist, an ex-assistant VP for the firm, told about "fraud parties" for the production of such physical records when he broke the story. He was quoted as saying, "The atmosphere of the party I attended was 'real happy', people would joke around, and we would make up funny names for doctors. . ."[24]

There was even an office in another building where a staff of people were supposed to be involved in the production of new policy applications.

Also, should an auditor have requested a written confirmation from a policy holder, the Equity staff "helped" him by providing names and addresses "at random" from the files. The "random" names turned out to be other loyal employees who dutifully filled out the forms and returned them to the auditor.

To appreciate how this might have all gone undetected requires some understanding of Equity's data processing operation. First,

---

[23]McLaughlin, R.A., "Equity Funding: Everyone Is Pointing at the Computer," Datamation 19 (June 1973): 88.

[24]Ibid.

"real" input to later master file updates.[23]

The major difference between the old legitimate records and the newly manufactured records was that a special department number was assigned (in this case department "99") that caused the records to be skipped over when it came to the billing cycle.

In most cases the fake records did not have to be supported by real paperwork. If an auditor ever asked to see the policy application, medical history, or other papers, he was put off long enough for someone within the company to generate some for him. Ronald Secrist, an ex-assistant VP for the firm, told about "fraud parties" for the production of such physical records when he broke the story. He was quoted as saying, "The atmosphere of the party I attended was 'real happy', people would joke around, and we would make up funny names for doctors. . ."[24]

There was even an office in another building where a staff of people were supposed to be involved in the production of new policy applications.

Also, should an auditor have requested a written confirmation from a policy holder, the Equity staff "helped" him by providing names and addresses "at random" from the files. The "random" names turned out to be other loyal employees who dutifully filled out the forms and returned them to the auditor.

To appreciate how this might have all gone undetected requires some understanding of Equity's data processing operation. First,

---

[23]McLaughlin, R.A., "Equity Funding: Everyone Is Pointing at the Computer," Datamation 19 (June 1973): 88.

[24]Ibid.

the EDP Department was a young one, established in 1969.[25] As the company grew in "sales" and "revenue", the EDP group was pressed to keep up. Bill Gootnick, Equity Funding Corp. VP for management information systems, stated, "You cannot compare it to old, established insurance company DP Departments that have evolved over the years. The oldest system we have may be three years old."[26]

Gootnick bristles over statements that the DP operation lacked controls. "The Equity Data Processing Division had the same controls that most installations our size would have had, including programmer project control, file retention, and report balancing. We're no different than 90% of the shops around."[27]

The Department is actually a division of the parent company rather than part of the life insurance subsidiary. It had a staff of about 75 and an IBM 370/145 which it ran in an open-shop service-bureau environment serving about 100 equity organizations, including several life insurance subsidiaries.[28] The actuarial department of EFLIC (Equity Funding Life Insurance Company) responsible for such things as annual reports, was just another open-shop user. The EDP staff screened run requested for legitimate account numbers to charge for the processing, then simply performed the services requested.[29]

---

[25] Ibid., p. 89.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

As soon as the state insurance regulators stepped into the operation, on March 30, both the IBM 145 and the IBM 513 were shut-down for a time. Frank Hyman (Manager of Systems and Programming) and Bob McGindley (a manager of Financial Systems), took it on themselves to issue a press release on behalf of the DP employees claiming the whole fiasco was a "people fraud" and not a "computer fraud". Both men claimed that EDP's only role was to lend "an air of authenticity to otherwise Bogus data."[30]

According to Hyman, the EDP Department was not in a position to see what was going on. There would have been no opportunity, for instance, to see that two year-end reports were in conflict. For one thing, he says, the reports were fractionalized, with one piece of the business appearing on one report, (which to the department was just another tape print) and another piece of the business appearing another day.[31]

Bob McGinley had charge of the systems that produce the general ledger. "There are 10,000 to 20,000 entries in the general ledger," said Bob. "My only responsibility is that it balances." On top of that, many of the entries that appear on the general ledger get there automatically from other sources like the Commissions System. Hyman said, "The general ledger system looks to see that entries have a legitimate account number . . ."[32]

Further, there was some evidence that the reports shown to

---

[30] Ibid.

[31] Ibid.

[32] Ibid.

the auditors were not even generated through the regular EDP department cycle. One incident that occurred just before word of the scandal spread, seem to uncover this evidence. An auditor asked the EDP Department to produce a report like the one he carried in. It did not have any of the report numbers used to control jobs, no titles, and no headers. When asked to produce another listing that would conform to the same business represented in the auditor's report, the total were, not surprisingly, different.[33]

California EDP Scandal

In a case that may be considered a classic of its kind, a California man siphoned off over one million dollars from the company where he was chief adminstrator and chief accountant.[34] Although his salary and bonus added up to $40,000 a year, he managed to supplement it handily at the rate of about two-hundred thousand dollars a year through a fascinating scheme which went completely undetected until he himself took steps to expose the losses. It was he who introduced the company to the use of electronic data processing through the services of an EDP Service company which he controlled, unknown to his superiors at the produce-growing and packing company where he worked.

Originally, he had intended only to conceal his lack of independence as the supplier of accounting support services. However, the opportunities for gain from this position were substantial. He soon began manipulating the recordkeeping operation

---

[33]Ibid.

[34]Jones, G. Hunter, "Leaking Financial Systems--Some Horror Stories," Journal of Accountancy 147 (May 1979): 87.

by overstating expense amounts and diverting these excess sums into checks payable to phony companies he had established.

Uncrackable Computer

In September of 1973, a computer operator on duty at Honeywell Information Systems, Inc. in Phoenix was startled to see the output printer on his console start up all by itself. Out rattled a message referring derisively to a recent Honeywell Press release about the company's vaunted new computer system called "multics". When it was done sniping at multics, the mysterious message signed off with the words "ZARF is with you again."[35]

ZARF was the code designation for part of a joint project of the U.S. Air Force and MITRE Corp., a defense-research outfit. The project is concerned with computer security, and a favorite pastime of people involved in it is cracking "uncrackable" computers. The day before the Honeywell computer acted up, the ZARF men, Air Force Major Roger Schell and Steven Lipner of Mitre, visited Honeywell to look over the security features of prospective systems for classified Air Force computing chores. After seeing the press release about Multics, Lipner quietly placed a long distance call to a ZARF colleague, Lieutenant Paul Karger, in Massachusetts, nearly 3,000 miles away. Karger, in turn, sat down at his teletypewriter computer terminal, dialed into Honeywell's private multics system, and typed in a few subtle instructions that subverted everyone of the system's safeguards, giving Karger effective control.[36]

---

[35] "Waiting For the Great Computer Rip-Off," Fortune 85 (July 1974): 143.

[36] Ibid.

The ZARF prank was particularly embarrassing because multics is designed with security as an uppermost consideration. Of all large commercial computers on the market, Multics probably incorporates the most elaborate safeguards against unauthorized tampering.[37]

Telephone Rip-Off

The first case of stealing a program from the memory of a computer over telephone circuits and a remote terminal in 1971 caused world-wide publicity, including three-inch headlines in the Paris Herald Tribune: "COMPUTER RAPED BY TELEPHONE."[38] It was the first case in which a search warrant was issued to search the memory of a computer for evidence. A programmer was convicted and given a suspended sentence for theft of a trade secret even though a witness in a related civil suit revealed that it was common practice for programmers in both companies involved to gain unauthorized access to the other's computer.

Research Study

The study analyzing the 160 recorded cases of computer abuse, (conducted by Donn B. Parker at the Stanford Research Institute) also included a description of an imaginary computer facility most vulnerable to computer abuse. The weaknesses are described below in descending order of importance, as organized by Donn B. Parker.[39]

1. The computer system is used for financial processing applications including payroll, accounts payable and receivable, and storage and maintenance of files of financial data. The

---

[37] Ibid.

[38] Parker, Donn B., and Nycom, Susan. "The New Criminal," Datamation 20 (Jan. 1974): 56.

[39] Ibid.

system puts out negotiable documents and takes in data representing negotiable documents. The system also stores and maintains other valuable data such as mailing lists and inventory of goods lists.

2. Among the employees, there is more mutual loyalty to each other than to the employer. The staff has more self-interest than interest in the success of the organization. Morale is low, and small groups join in defensiveness toward management and society. Employees reinforce one another in rationalizing acts that management would not condone.

3. The organization does not separate sensitive job functions and lacks dual control of important tasks. Most serious is the nonseparation of application programming, program testing, systems programming, data input and output handling, customer servicing, materials storage, and computer operation. Separation is missing in tasks, responsibilities and physical access.

4. The system services and physical facilities are available to some employees during nonworking hours and without supervision. The absence of responsible staff in nonbusiness hours is not compensated for by sufficiently increased physical security.

5. Computer programs, including the operating system, are not under modification control, and ownership is not sufficiently displayed or otherwise established. Programs do not include sufficient controls, tolerance checking and anomaly testing. Exception reports produced during processing contain little information indicating unauthorized activity, but contain volumes of useless data that burden the auditor beyond his comprehension and attention span.

6. Disgruntled employees are not identified and removed from sensitive jobs. Employees being released from positions of trust are not immediately removed from their work areas and positions of system access. Use of computer facilities, materials and services is not monitored or sufficiently controlled.[40]

Undetected Computer Frauds

One cannot help inferring that a significant amount of fraud and embezzlement goes undetected. According to one security expert "Almost all computer-assisted fraud is so simple and straightforward that it makes you wonder what the really smart (and as yet undetected) people are doing?"[41]

Since so many cases are uncovered only by chance or because the perpetrator simply gives up or makes a stupid mistake, one may well conclude that most fraud goes undetected. This is believed to be true for computer fraud as well. Furthermore, it is possible to determine the most likely undetected cases simply by applying the pattern of noncomputer-related frauds to computer users. Other cases appear probable, considering the buying, selling, employment or functional activities of various types of organizations.[42]

First, it should be clear that a large number of undetected computer frauds simply follow the patterns found in these detected cases. Thus, there is probably undetected corporate inventory and

---

[40] Ibid.

[41] Allen, Brandt. "Computer Fraud," Financial Executive, May 1971, p. 41, Quoted in (or "Cited By") Stone, Robert. "Who is Responsible for Computer Fraud?" Journal of Accountancy 139 (Feb. 1975): 36.

[42] Allen, Brandt. "The Biggest Computer Frauds," Journal of Accountancy 143 (May 1977): 57.

disbursements fraud, undetected welfare fraud in federal, state and local government agencies and many undetected funds transfers in banking institutions.

In order to categorize the assumption that there could possibly be some undetected cases of computer abuse, Brandt Allen of Colgate Darden Graduate School of Business Administration, put these possible frauds into the following six classes.

> 1) Pension Frauds. There were a couple of cases where pension payments were discovered being made in the names of deceased individuals. But the number of pensioners in this country, the number of pension-paying organizations and the ease of the scheme suggest that computerized pension fraud in the United States is a hidden problem of major significance. There are probably thousands of deceased pensioners on computer files whose monthly checks are being diverted to white collar criminals.
>
> 2) Inventory and Disbursement Frauds in State and Local Governments. Disbursements and inventory frauds were found to be big problems for automated systems in corporations and federal government agencies; the same must be true for state and local governments. When you consider the number of state and local governments in existence, the amount of purchasing they do and the size of their inventories, this must be considered another hidden problem.
>
> 3) Insurance Claims Fraud. From the cases to date it might be concluded that there is no computer-related fraud in insurance companies. This cannot be so. The nature of the business in this industry is money collecting, investing and paying; there are many individual accounts, many transactions, a high degree of automation the dollar magnitude is high and much of the industry depends primarily on good faith--such as medical insurance claims processing. Few industries have such a high potential for computer fraud and so few detected cases to date.
>
> 4) Corporate billing frauds. While there were a few detected cases of this type, the total is surprisingly small considering the vast amount of billing activity in the corporate sphere. The large number of employees who have access to billing transactions

> and the ease of manipulation suggest that much fraud here goes undetected, particularly that affected by deleting, blocking or altering transactions.
>
> 5) Federal Government Program Funds. According to the reported cases of computer fraud, there have been no dishonest computer programmers in the federal government. This hardly seems possible. Considering the potential for abuse in such agencies as the Department of Health, Education, and Welfare, the Department of Defense, the Internal Revenue Service and the Agriculture Department and in programs such as revenue sharing, it may be concluded that a significant number of payment frauds generated by unauthorized program patches go undetected in the federal government.
>
> 6) Loan Frauds in Commerical Banks. Commercial banks, as opposed to savings institutions, also appear surprisingly clean. For many reasons, the chances of operating successful funds transfers are lower for demand accounts than for savings accounts, but the opportunities for loan frauds are greater in commercial banks. It seems impossible that computer-assisted loan frauds are not a giant program for commercial banks. My guess is that many are out there waiting to be detected.[43]

However, it is almost impossible to completely reduce abuse in a computer facility. It is inevitable from the cases sited above, that more precautionary steps could be implemented to reduce the risk of computer abuses.

Thus, it was the purpose of this chapter to create an awareness of the possible dangers inherent in a computer system. In so doing, this chapter cited cases of computer abuse. Next, this chapter discussed the six major classes in which computer abuse may fall. Then this chapter brought up the assumption that there could be a great many cases of computer abuse still undetected.

---

[43] Ibid.

CHAPTER IV

The objective of this chapter is to discuss the audit implications the computer or EDP system has placed on the accounting profession and some possible procedures to consider while engaged in an audit of an advanced EDP system.

In order to accomplish this objective the following areas will be discussed. First there will be a discussion of the auditing standards as they relate to advanced EDP systems and some questions that could be asked about the effect EDP is placing on those standards. Second, a discussion on possible control methods that could be utilized when implementing an EDP system. Next a discussion on the impact advanced EDP systems have had on auditors, EDP personnel and vendors. Then a discussion will follow on possible audit procedures and techniques.

Auditing Standards and Advanced EDP Systems

The normal objective of the examination of financial statements by the independent auditor is the expression of an opinion on the fairness with which they present financial position, results of operations and changes in financial position in conformity with generally accepted accounting principles.[44] This objective remains unchanged whether or not EDP is in the

---

[44]Statement on Auditing Standards (SAS) No. 1, "Codification of Auditing Standards and Procedures," AICPA (New York: 1979), Section 110.01.

accounting process, including the preparation of the financial statements being examined.

The auditor's report states whether the examination has been made in accordance with generally accepted auditing standards.[45] The application of the standards of reporting does not change when EDP is used. The application of the other standards, however, can be affected by EDP. This section will discuss the significance of EDP to the application of auditing standards.

Technical training and proficiency are covered by the first general standard, which states "the examination is to be performed by a person or persons having adequate technical training and proficiency as an auditor."[46]

When EDP is used in the accounting process, the auditor should possess a level of EDP proficiency. When sophisticated systems are used, the auditor may choose to rely on EDP specialists; however, the auditor should possess a level of proficiency in EDP sufficient to permit adequate supervision of these specialists. Higher levels of EDP proficiency will be required for auditing advanced EDP systems. Specialists will be used to a greater degree.

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.[47]

---

[45] Ibid., Section 410.01

[46] Ibid., Section 210.01

[47] Ibid., Section 320.01

The study and evaluation embraces the following three phases: 1) Reviewing Controls. The auditor's review includes the structure of accounting control within the entire accounting system. Understanding the manner in which accounting information flows through the system is fundamental to the auditor's evaluation of accounting controls and to the design of other auditing procedures. The auditor will be concerned with the role of EDP in the accounting process.[48] The ability to follow the flow of accounting information through the system, normally called an "audit trail", is of particular concern to the auditor in an EDP system.

Future systems will become more complex and will use sophisticated information processing and control techniques. This will create some special problems in gaining an understanding of the system:

> Will system documentation suitable for audit use be available?
>
> Will the auditor be consulted early enough in the systems design process to effectively influence the audit-related aspects of proposed systems?
>
> Will adequate audit trails be provided?
>
> If traditional audit trails prove too costly, will acceptable alternatives be developed?
>
> Who will develop the alternatives?
>
> Will systems become so complex that the cost of reconstructing or auditing a sequence of events becomes prohibitive?[49]

The introduction of EDP into the accounting system creates some additional control considerations. Typically, accounting

---

[48] "Advanced EDP Systems and the Auditor's Concern." Journal of Accountancy 139 (Jan. 1975): 69.

[49] Ibid., p. 70.

control functions, which were performed by separate individuals in a manual system, are concentrated in an EDP system. Basic accounting records may lose their visibility and now can be altered without leaving a trace. Records may be accessible to programmers, operators, systems personnel and, in some situations, to users whose activities are evaluated in terms of the data in the records. The use of EDP in an accounting system, therefore, requires the design and implementation of control procedures to assure effective accounting control.

After the auditor obtains a general understanding of the entire system of accounting control, he is able to consider whether he will rely on the EDP accounting controls as a basis for restricting other audit procedures. Depending on the circumstances, this decision may be made for all or individual applications and will be based on both the adequacy of the EDP accounting controls and the audit efficiency obtained by reliance on them.

In advanced EDP systems, the nature of accounting controls will change and their importance will increase. Some related questions follow:

What can the auditor do to assure that adequate controls are provided for within the system?

Will the auditor be forced into a position of almost total reliance on accounting controls at the expense of other auditing procedures?

What is the potential effect on accounting controls if client personnel are inadequately trained in the use of the system?

When systems extend outside the business enterprise, how will the auditor review controls?

Will auditable controls be provided over changes to the system and programs?[50]

2) Testing of Compliance. The purpose of tests of compliance is to provide reasonable assurance that the accounting control procedures are being applied as prescribed.[51] In a manual system. the auditor examines evidence, such as approvals and audit stamps, that indicates whether the control procedures were, in fact, functioning during the period covered by the financial statements being examined. Similarly, in an EDP system, the auditor seeks assurance that the control procedures are functioning during that period; however, this assurance is frequently obtained in different ways. For example, the auditor may use a test deck or file developed under his control to test programs that process sales transactions in order to determine if variations from the company's stated credit policy will be detected and reported for corrective action.

Test of compliance will become systems dependent in an advanced system. Some as yet unanswered questions are:

What new techniques will be required?

Will the auditor be able to obtain assurance for the entire period under examination?

Will "on-line auditing" become a widespread approach?[52]

3) Evaluating Controls.[53] The auditor considers the nature of the accounting system, the adequacy of prescribed accounting controls therein and the degree of compliance with those controls

---

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] Ibid.

in making an evaluation to determine the extent to which auditing procedures may be restricted. These auditing procedures are generally directed at obtaining evidence supporting the reasonableness of transactions and balances in the financial statements.

Evidential Matter

The third standard of field work states; "sufficient competent evidential matter is to be obtained through inspection, observation, inquiries and confirmations to afford a reasonable basis for an opinion regarding the financial statements under examination."[54]

Evidential matter supporting the financial statements consists of the underlying accounting data and all corroborating information available to the auditor. This includes documentary material such as checks, invoices, contracts and minutes of meetings; confirmations and other written representations by knowledgeable people; inspection and physical examination; and other information developed by, or available to, the auditor permitting him to reach conclusions through valid reasoning.

EDP typically changes the nature of the underlying accounting data and, to a certain extent, can affect the nature of the corroborating evidential matter. For example, when accounting data is maintained only in machine sensible form, the auditor may request that it be printed out in its entirety for audit review and testing. Alternatively, the auditor may use the computer to assist in the examination of these records. This audit use must, of course, be performed independently.

---

[54]Statement On Auditing Standards (SAS) No. 1, "Codification of Auditing Standards and Procedures," AICPA (New York: 1979), Section 330.01.

The computer may also be used to develop analytical information useful to the auditor.

Traditional independent evidence, such as copies of invoices and purchase orders, is being replaced by computer-prepared records in advanced systems. The records are in electronic form, and, therefore, cannot be inspected in the traditional fashion. This fact creates some further questions:

> What alternative approaches can be developed?
>
> What steps will have to be taken to ensure that the data the auditor requires will be available when needed?
>
> What alternative forms of evidence will be available?[55]

Security

What does security in the EDP environment have to do with the auditor's responsibilities in evaluating internal control? A great deal! Without security and the safeguards provided by a program of security, the controls in the EDP activities could be ineffective.

"Resources are exposed to two types of hazards: natural, like fire, wind, rain and flood; and of human origin, like accidents, omissions, conversions, misappropriations, theft, and mischief."[56] A security program must be designed to protect resources from loss by either accidental or intentional means. Furthermore, the cost of guarding against each of the factors must be weighed against the

---

[55]"Advanced EDP Systems and the Auditor's Concern." Journal of Accountancy 139 (Jan. 1975): 71.

[56]Bund, Melvin. "Security in an Electronic Data Processing Environment." CPA Journal 45 (Feb. 1975): 34.

risks entailed. It therefore becomes management's responsibility to decide what to protect (data files, programs, equipment, facilities, personnel) and under what circumstances to protect it (against which natural hazards or hazards of human origin).

It has been determined by IBM Corporation Studies[57] that most of the hazards (about 95%) consist of:

-- error and omission (accidental)
-- water (faulty plumbing)
-- defalcations (deliberate, rational acts)
-- fire (to the actual equipment or to the area)
-- disgruntled employees (irrational acts)[58]

All other types of hazards combined cause less than 5% of situations encountered.[59]

Accordingly, it becomes a necessary business (management) judgement to evaluate exposure to risk, by assigning a negative value to the exposure of specific resources.

Exposure involves two factors:

1) probability of loss, and
2) expenditure to repair, replace, or recover.[60]

Thus, exposure is measured and compared with the acceptable level of risk. Management decisions in this area may vary between organizations and even levels of management; but they always involve comparisons between the cost of protective measures and the exposure. Alternatives may be evaluated on the basis of relative levels of residual risk that remain after installing protective devices and

---

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] Ibid.

procedures.

Protective Measures

Protective measures are of several kinds. Some involve physical safeguards for the premises against burglary, fire, and other damage. Additional protective measures involve recovery and backup to forestall loss of information, protect records, or operate under emergency conditions. Finally, protective measures can involve controls and procedures for separation of responsibilities, machine room operation, and audit.

The controls and procedures discussed above can be incorporated in software and/or hardware. Access to programs will have some control features and procedures should establish accountability for program use. Hardware features should control operation of equipment by preventing unauthorized access to terminals. Access to specific data should be limited to designated individuals only.[61]

The rapid advances of computer technology have created both new challenges and new methods for protection of data. In the beginning, the basic concern was to protect against unintentional omissions and errors. Now the emphasis has shifted to a degree, in recognition of the possibility for disruption of data files by disgruntled employees. Irrational acts of this type are more difficult to guard against than inadvertent mistakes.[62]

Principles of a Secure System

Security of a data processing system depends on a separation of

---

[61] Ibid.

[62] Ibid.

be meaningless unless some other data disclosing employee name or position were known. Also, if a coded situation were identified without the key to the code, the information probably would be meaningless.

-- Time is a factor in sensitivity. Yesterday's payroll register would be meaningful, but one of five years ago would probably be of no sensitive value today. However, it should be noted that some items do increase in sensitivity with age.

-- Sensitivity is related to the degree of interpretation of the data. Data tend to be more easily understood when they are organized and conclusions are given.[64]

Functions of a Secure System

Security functions apply to all points of interface with other systems. They must be operative at every point where a user has contact with data, either through the equipment or external to it. Several practices are involved.

-- Limiting access to data to authorized persons, and even then only to those data that are needed.

-- Control by the process itself over its own domain.

-- Accountability of individuals.

-- Reporting variances to responsible management so as to permit timely and appropriate corrective action.

-- Presentation of a threshold of usability. The controls, in deterring or controlling or limiting improper usage, should not be such that it becomes impossible to work or live with the system.[65]

Six basic factors in implementing the security of the data and the system become evident:

---

[64] Ibid., p. 35.

[65] Ibid.

1. Identification - name or other description.
2. Authentication - an ID card, photo, etc.
3. Authorization - including an indication of the authorized job.
4. Delegation - evidence of right to use by the proper manager.
5. Audit trail - chronological listing of tapes used and released.
6. Surveillance - tape counts and other monitoring devices as to usage.[66]

Impact of Advanced EDP Systems on the Auditor:

The general audit implications of advanced systems, and some approaches for dealing with these implications can be summarized in the following paragraphs.

Businesses are becoming more dependent upon and are demanding greater use of the computer. As a result, EDP systems development may be based upon unproven or inadequate internal control techniques. Therefore, guidelines and standards will have to be developed to ensure that future systems contain the basic elements of good internal control.

It is more difficult to control and understand the effects of an individual transaction in complex systems. Further, it is becoming more difficult to prove the integrity of complete transactions. Therefore techniques to control the integrity of data in an EDP system must be developed.

The audit trail, in its conventional form, may no longer exist. The traditional documents and magnetic data that comprise the audit trail may not be present and/or may take on a whole new dimension. Alternative approaches will therefore be required.

The auditor will have to develop procedures to ensure that

---

[66]Ibid.

the system subject to the audit test is the same as the one used to produce the financial statements.

New control methods to ensure the security and integrity of data, including changes to systems and programs, must be developed.

The auditor will have to keep informed about future developments in systems and technology, anticipate the audit impact of these changes and implement the audit techniques and software needed to cope with these developments.

The auditor must still be able to perform the audit at a reasonable cost. This will be a challenge to the auditor's technical skill and ingenuity.

Audit Impact of Advanced Systems on EDP Personnel

The following implications have been discussed, in general, throughout this chapter. Those items that directly affect EDP personnel are:

1) Disappearance of source documents. The auditor will need assistance in dealing with the situation.

2) Interface with the users. The unsophisticated user should be able to understand the capabilities of the system.

3) Need for documentation. The system should be supported by complete documentation suitable for audit use.

4) Usable audit software. Audit software should be used for information retrieval and audit operations on an independent, controllable basis.

5) Records of system changes. There is a need for an independent tracking system for program changes. Auditors should

be kept informed about revisions.

6) EDP personnel should give serious thought to how computer based auditing can be accomplished at a reasonable cost. This should be evaluated during all phases of systems design.

7) Lack of audit trail. The system should be able to retrieve the elements of a transaction at a relatively low cost. This should include the ability to retrieve transactions that may, for security and backup purposes, be considered out of date but that are still required for the audit.

8) Audit control requirements. The auditor should be able to assure himself that the independent functioning of this program has not been compromised. This will require the use of new techniques.[67]

Audit Impact of Advanced Systems on Vendors

The vendors of computer hardware and software can assist the auditor of an advanced system. Some factors to consider are:

1) Design of future systems should include the following basic controls over hardware and software: a) standardized control features and capabilities, b) controls that restrict the user's ability to modify or circumvent built-in controls and c) the capability to maintain an independent log of programs processed on the system and data introduced through the computer console.

2) Design of future systems should consider the need for the following audit capabilities: a) a system testing package that can assure that standardized controls are functioning properly, b) the

---

[67] "Advanced EDP Systems and the Auditor's Concern." Journal of Accountancy 139 (Jan. 1975): 71,72.

capability to independently monitor certain system actions, c) the capability to isolate and "tag" a transaction from the time it is introduced into the system until the time that processing is complete and d) a program that could review all other programs and data changes and verify that the data base has been correctly updated according to predefined parameters.

3) Vendors should provide education on new systems for auditors to allow them to evaluate the audit effects of technological changes.[68]

Possible Audit Procedures and Techniques

Although it is possible to suggest some approaches and solutions, it should be understood that a great amount of further research by vendors, users and auditors will be required to develop definitive solutions for the problem areas indicated. Therefore, the following techniques are just a few of the many possible techniques available to the auditor.

The auditor's involvement in system design. The auditor's participation in the system design will become more critical in the case of an advanced system. This involvement will enable the auditor to provide a valuable contribution, particularly from the control standpoint to the company's new systems and will, since audit requirements can be specified during the initial phase, decrease the chance of an "unauditable" system being developed.

Integrated test facility (ITF). The ITF technique (sometimes referred to as the mini-company approach) involved establishing the capability of introducing selected input into a system simultaneously

---

[68] Ibid., p. 72.

with live data, and tracing the flow of transactions through the various functions in the system. The object is to permit auditors to (1) enter an EDP system under normal operating conditions, 2) test transactions for which the results have been predetermined, and 3) compare the results actually produced to the predetermined results.[69]

Since the use, as opposed to the development of the ITF technique does not require an extensive understanding of computer technology, the technique can be readily used by both the external and internal auditor, regardless of their backgrounds in electronic data processing.

Computer to computer confirmation. The input to one company's computer system may be provided by direct output from another company's computer. In this situation, certain types of information could be confirmed directly between computer systems. This technique requires the design of software to perform such a function, which can be a difficult task. But, once developed, it would facilitate the preparation of more timely confirmations because of the speed of the computer.

Tagging of transactions. Tagging is used to trace live data through the system. As each processing step is performed, the interaction of the selected transactions with other data and related tests is displayed. Printouts may be produced to assist the auditor in tracing the transactions. Or, the auditor may receive this information at a terminal located in his office. Again, the auditor could be performing a significant portion of the audit during the fiscal

---

[69]Chaiken, Barry R., and Perry, William E. "Accounting and Auditing," Journal of Accountancy 135 (Feb. 1973): 74.

year.[70]

Generalized audit software. The use of generalized audit software by auditors permits independent verification of arithmetic totals, identification of unique characteristics within the data files and a wide variety of other audit tests to be performed on a post audit, or after-the-fact, basis. The use of audit software does not require the auditor to be proficient in computer programming languages in order to prepare special audit reports or perform calculations using the computer.

The main advantage of the use of generalized audit software by the auditor is independence. He can independently use the speed and accuracy of the computer to help with the audit of data. He need not rely on others with more programming knowledge to program his audit needs.[71]

The purpose of this chapter was to give an overall picture of the implications that the computer has placed on the accounting profession. In so doing, this chapter presented the standards that affect advanced EDP systems and some possible questions that might be asked when considering those standards. Then a few possible control procedures were presented. Next a discussion followed on the impact EDP had placed on the auditors, EDP personnel and vendors. Finally a discussion on possible audit procedures and techniques was presented.

---

[70] "Advanced EDP Systems and the Auditor's Concern." Journal of Accountancy 139 (Jan. 1975): 71.

[71] "A Survey of Audit Software," Journal of Accountancy 134 (Sept. 1972) 39-66, Quoted in (or "Cited By") Harlan, Stephan D., and Rittersback, George H. "Auditing Advanced Systems," Journal of Accountancy 137 (June 1974): 84.

CHAPTER V

CONCLUSION

The purpose of this paper was to establish a better understanding of the effects that computer technology is having on the auditing profession. The reason is that auditors are becoming more and more affected by the existence of computers within accounting information systems.

In an attempt to reach the above objective, this paper presented many things. A discussion on how computers help to facilitate the information process and why auditors should be concerned with the information system. Matters of concern and potential problem areas dealing with computer abuses have been identified. Questions concerning auditing standards as they relate to advanced EDP systems have been presented. Also attention was given on the audit impact of advanced EDP systems on auditors, EDP personnel and the vendors.

Hopefully, by presenting the above areas of concern, this paper has conveyed the growing importance of computers in the audit function. One reason to consider is that computers are altering the audit trail and causing auditing procedures to change. Therefore, it is imperative that auditors be aware of how computers are affecting their profession.

SELECTED BIBLIOGRAPHY

BOOKS

1. Carroll Archie B., and Watson, Hugh J. Computers for Business (Dallas: Business Publications, 1976).

2. Davis, Gordon Bitter. Auditing and EDP. (New York: AICPA, 1968).

3. Lott, Richard W. Auditing the Data Processing Function. (New York: Amacom, 1980).

4. Roy, Robert H., and MacNeil, James J. Horizons for a Profession; The Common Body of Knowledge for Certified Public Accountants. (New York: AICPA, 1967).

5. Sanders, Donald H. Computers in Business. 4th Ed., (New York: McGraw-Hill, 1979).

6. Statement on Auditing Standards (SAS) No. 1, "Codification of Auditing Standards and Procedures." (New York: AICPA, 1979).

PERIODICALS

1. Allen, Brandt. "Danger Ahead! Safeguard Your Computer." Harvard Business Review 46 (Nov.-Dec. 1968): 97-101.

2. Allen, Brandt. "The Biggest Computer Frauds." Journal of Accountancy 143 (May 1977): 52-62.

3. Brown, Foster. "Auditing Control and System Design." Journal of Systems Management 26 (April 1975): 24-31.

4. Bund, Melvin. "Security in an Electronic Data Processing Environment." CPA Journal 45 (Feb. 1975): 33-35.

5. Chaiken, Barry R., and Perry, William E. "Accounting and Auditing." Journal of Accountancy 135 (Feb. 1973): 74-78.

6. Collins, Stephen H. "News Feature." Journal of Accountancy 144 (July 1977): 34-35.

7. Davis, Gordon B., and Rittenberg, Larry E. "The Roles of Internal and External Auditors in Auditing EDP Systems." Journal of Accountancy 144 (Dec. 1977) 51-58.

8. Davis, James R. "EDP Control Means Total Control." Management Accounting (NAA) 58 (Jan. 1977): 41-44, 47.

9. Freed, Roy N. "Computer Fraud--A Management Trap." Business Horizons 12 (June 1969): 25-30.

10. Green, Jeffrey D. "Systems Documentation, Internal Control, and the Auditor's Responsibility." CPA Journal 44 (July 1974): 25-28.

11. Harlan, Stephan D., and Rittersbach, George H. "Auditing Advanced Systems." Journal of Accountancy 137 (June 1974): 83-85.

12. Horne, John M. "EDP Controls and Check Fraud." Management Accounting (NAA) 56 (Oct. 1974): 43-46.

13. Hubbert, James F. "Computer Personnel Frauds." Journal of Accountancy 148 (Aug. 1979): 44, 46, 50.

14. Jones, G. Hunter. "Learning Financial Systems--Some Horror Stories." Journal of Accountancy 147 (May 1979): 87-90.

15. Mason, Jr., John O., and Davies, Jonathan J. "Legal Implications of EDP Deficiencies." CPA Journal 47 (May 1977): 21-24.

16. McLaughlin, R.A. "Equity Funding: Everyone Is Pointing at the Computer." Datamation 19 (June 1973): 88-89, 91.

17. Parker, Donn B., and Nycom, Susan. "The New Criminal." Datamation 20 (Jan. 1974): 56-58.

18. Schneidman, Arnold. "Need for Auditors Computer Education." CPA Journal 49 (June 1979): 29-31, 34-35.

19. Stone, Robert. "Who is Responsible for Computer Fraud?" Journal of Accountancy 139 (Feb. 1975): 35-39.

20. Stone, Robert. "Some Security and Integrity Controls in Small Computer Systems." Journal of Accountancy 141 (Feb. 1976): 36, 38, 40.

21. Thorne, Jack F. "Control of Computer Abuses." Journal of Accountancy 138 (Oct. 1974): 40, 42, 44, 46, 48, 50.

22. "Advanced EDP Systems and the Auditors Concern." Journal of Accountancy 139 (Jan. 1975): 66-72.

23. "Computers Rush Into Your Daily Life." U.S. News and World Report 71 (Nov. 5, 1973): 45-47.

24. "On the Coast-to-Coast Trail of Equity Funding." Business Week, April 21, 1973, pp. 68, 70, 72.

25. "Statement on Auditing Standards No. 3--The Effects of EDP on the Auditor's Study and Evaluation of Internal Control." Journal of Accountancy, 139 (Feb. 1975): 72-76.

26. "Waiting for the Great Computer Rip-Off." Fortune, 85 (July 1974): 143-146, 148, 150, 152.