5-1974

Internal Control Techniques to be Considered When Installing a Computer System

Donna Dietz

INTERNAL CONTROL TECHNIQUES TO BE CONSIDERED WHEN INSTALLING A COMPUTER SYSTEM

by
Donna K. Dietz
Bachelor of Science, North Dakota State University 1971

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 Science

Grand Forks, North Dakota
May 1974

TABLE OF CONTENTS

INTRODUCTION

Although no longer a new phenomenon in the business world, computers are still somewhat mysterious to many people in management. As a result, many of the physical and operational controls and safeguards that existed in manual systems and could have been carried over or adapted, have been weakened or eliminated. Moreover, in too many cases, little has been done to institute new, effective controls to protect computer-based operations and records.

The result has been disastrous. To site just a few examples:

> An employee of the New Jersey National Bank electronically siphoned $128,000 out of 33 of the bank's accounts and into the balances of two outside accomplices. The trio were caught because the bank switched to new computers that did not give the 'inside man' time to erase the withdrawal data from the defrauded customers' bank statements, as had been planned.

> Jerry Schneider, a 21 year-old UCLA engineering graduate, studied Pacific Telephone and Telegraph's computer by posing first as a journalist and later as a customer. He learned enough to place commercial orders for telephone equipment simply by punching the right beep tones on his touch telephone. He then picked up the equipment and sold it through a dummy firm. Incredibly, the telephone company let his unpaid bills accumulate for three years. The LosAngeles district attorney charged that Schneider stole $1,000,000 worth of goods...[1]

> A chief teller at a branch New York's Union Dime Savings Bank stole $1.5 million over three years by manipulating inactive accounts in the bank's computer. He was caught by accident when police, while working on a gambling case, raided a bookmaker and found records showing the teller had been betting as much as $30,000 a day.[2]

Perhaps the most spectacular recorded example is the Equity Funding scandal. Dummy life-insurance policies worth millions of dollars were

programmed into the company computers. The business operated on these "assets" for years. When discovered the company went into bankruptcy.

These are just a few of the recorded cases of manipulating a company's computer. There are thousands more recorded cases and no one can guess how many costly errors have gone undiscovered. The majority of these errors could have been prevented if a control system had been installed.

Control systems for computers have four major objectives: to ensure that all data are processed, to ensure that the correct data are processed, to ensure accurate and timely processing of the data, and to assist in determining the cause of errors when inaccurate processing occurs. This paper is presented as a guide for management for becoming aware of the controls which are useful and appropriate for application to a computer system.

FOOTNOTES

[1] "Key Punch Crooks," Time, (December 25, 1972).

[2] Kenneth S. McReavie, "A Conceptual Approach to Computer Controls, Management Controls, (July 1972):166.

PART I

DATA CONTROLS

The input and output functions of a computer system are man's communication link to the central processing unit (CPU). A central processing unit that is functioning perfectly will not give man accurate data if the data put into the CPU is not correct. Therefore, controls must be established over both input and output. In this part, controls will be discussed to insure that all valid data reaches the CPU and, after processing, all valid data reaches man. Chapter 1 will discuss input controls and controls over output will be discussed in Chapter 2. Controls over error investigations and corrections will be considered in Chapter 3.

Chapter 1

Input Controls

Source data for the computer is generated from the operating departments. Input controls ensure that all valid data are being processed. They also provide a way for the computer to check summary processing accuracy. Many of the controls discussed in this chapter are not new; they are merely adapted to fit a computer-oriented data processing system.

The most common technique for ensuring that all valid input is received is to compare two independently derived batch totals. One batch total is accumulated by the computer; the other batch total is manually determined prior to the computer processing. Usually the manually determined totals are accumulated on adding machines or by manual count at the control desk. (The control desk will be discussed in a later chapter.) This batch total can be put into the computer for comparison.

An additional method of ensuring all data are received is to start a new batch numbering sequence for each processing period. Batch numbers may be assigned in ascending sequence. A missing batch number would indicate an omission of data.

For systems which do not use batch processing techniques, methods are required to ensure that all valid input is processed. A confirmation or acknowledgement message may have to be sent to the control point (a control desk or the source of the data) for each input transaction. A control is then required to assure that confirmations are received for all input transactions.

Systems without batch processing are more costly to control than batch systems since action is required to confirm that each transaction is received. Also, since in most cases a comparison of the confirmation notice and the original input is completed manually rather than by the computer, the reliability of these systems is more subject to human error.

The use of serial numbered forms is an inexpensive control feature. This practice is certainly not new, but is included because of the computers ability to control serial numbers. Serial numbers of certain documents which constitute input (such as requisitions, vouchers, and receipts, as opposed to invoices and checks) might be introduced along with account codes, quantities, etc., and stored within the computer. At periodic intervals the serial numbers of those documents which had not as yet passed through the data processing unit could be determined by the computer for review and follow-up. This would assure that all data are being processed through the computer facility.

Peripheral devices are available which ensure the accuracy and validity of all input data. Although many digit verification devices are not associated electronically with the EDP system, this equipment is just as much a part of the system as is the electronic computer and its components. One machine, the International Business Machine's 56 Verifier, checks and verifies card-punching. The operator, using the original source documents and the punched cards, rekeys the data into the keyboard of the Verifier. The machine compares what has been punched and what is rekeyed; any difference will cause the keyboard to lock. Another digit verification device is National Cash Register's Check Digit Verifier. This machine is designed to test the validity of an account number before it is recorded into tape or cards by means of a programmed mathematical formula. One, or a combination, of these de-

vices improves the controls of the input.

An alternative to key punching of cards is the magnetic tape encoder. This device can be used to record data and to verify it. The data is not written on tape until an entire record has been keyed in. Any error the operator notices may be corrected immediately. The verification process includes the correction of errors.

Verification is a duplicate operation and therefore doubles the cost of data conversion. Various methods are used to reduce the amount of verifying. One method is to verify only part of the data. Some data fields are not critical and an error will not affect further processing. Examples are descriptive fields containing vendor name, part description, etc. which under most circumstances are not critical. Prepunched cards and stubs, as well as duplication of constant data during keypunching will help to reduce verification. Turn-around documents reduce the need for keypunching and, therefore, key verification. "In a billing operation, for example, a punched card is used as the billing document. The customer is asked to return the punched card (or a punched stub) with his payment. If the customer makes a full payment, no key punching may be required; if partial payment is made, the amount of the payment is punched, but verification is not necessary for any fields other than the amount."[1]

Another method to reduce key verification is to sample check each operator's work. If her error rate is below a predetermined acceptable level, no verification is made; if it is not, complete verification is made.

Verification can also be conducted by visual inspection of the printing on the card or a visual review of a listing of the cards. Other procedures, such as a check digit or a batch control total, may be substituted for machine verification.

Other controls, such as record count and tape labels, also help to ensure that all valid data are being processed. (These controls are discussed in Part II.) The procedures are much the same as the controls used in a non-computer oriented accounting system. They have been adapted to fit into a system of electronically run machines.

FOOTNOTES

[1]Gordon B. Davis, Auditing & EDP, (New York, American Institute of Certified Public Accountants, 1968):61.

Chapter 2

Output Controls

Controls over input data and processing give a high degree of assurance that the computer output is correct. Output distribution should be controlled to ensure that those, and only those, authorized to receive the reports (or other output) do receive them. Persons receiving the output form an important error detection control point, so provisions should usually be made in system design for error feedback from recipients of output.

The output should be reviewed before it is sent from data processing. The person charged with processing control inside the data processing department checks for completeness of output, correct numbers of copies, agreement of control totals, and also cross checks with output from related programs. This review prior to distribution includes scanning of the output for obvious errors, such as lines of meaningless characters or missing fields.

It may be desirable to have additional tests performed on the output before accepting it. These tests are usually either reasonableness tests using approximations developed independently of data processing (total statistical tests) or comparisons with independently maintained control figure.

Persons using output frequently detect errors. These employees should not redo the processing to detect the errors, but should apply a visual reasonableness test.

The documentation for a run specifies the number of copies to be prepared by the computer operator. Multiple copies must be separated and the carbons removed (decollation). Continuous forms are sometimes separated

(burst). Mechanical equipment is available for removing the carbons and separating the individual sheets.

The documentation generally describes the distribution of the output. A report distribution sheet should be used to record the distribution of the output. A transmittal or release form may be attached to the document; this form is especially necessary if the output contains confidential information.

Controls over the output of the computer system give another assurance that all valid information will be received by those persons or departments authorized to receive them.

Chapter 3

Control over Error Investigations and Corrections

Computer installations normally try to have programs written so that errors will not halt processing. (Sequence and control-total errors require that processing be aborted, but other errors should not halt processing.) An error procedure written into the program usually provides for a temporary halt--for error identification and listing to facilitate subsequent follow-up--and then a continuation of processing. However, before logging out such a transaction, the program should process it through all remaining error tests. The procedure followed in any particular case depends on the nature of the errors detected. It is not usually considered good practice to have the operator initiate data corrections.

If there are errors in input data, an input error listing or report (log) which explains the reason for each rejected item should be prepared. The rejected data and the error report should be returned to the originator for correction and resubmission. Personnel receiving the error reports should be instructed in the handling of them. The data processing organization may make a follow-up check for resubmission or they may leave the responsibility for correction and resubmission entirely to the originator. In either case the responsibility should be defined specifically. The person designated to correct errors should do so within a set time limit. Certain types of erroneous data became critical to the operation of the system and will need immediate action. Other types of errors that might enter the system are not so critical and corrections can be reentered the following day or week.

When faulty records are detected, one method of ensuring correction is to write the faulty records on a suspense file for subsequent analysis. A suspense file is simply a collection of all erroneous records which have been rejected. When erroneous records are resubmitted and accepted, the record is removed from the suspense file. This technique provides a running total of the rejected items not yet corrected.

Another method is to flag the faulty items but leave them in the file. An error in control totals may be handled through a suspense entry which temporarily corrects imbalances between debits and credits or between control totals. If there are dummy or suspense records maintained in the file to hold balancing entries or unmatched items, such items should be identified clearly and the purpose of each should be investigated promptly.

Master file changes, such as changes in employee pay rates, customer credit limits, etc., should be closely controlled. All master file changes or changes in program data factors should be authorized in writing by the department initiating the changes. A notice or register of all changes should be furnished to the initiating department to verify that the changes were made and to subject the changes to their review.

If an error suggests a faulty program, correction is usually made through a formal request for a programming change. After approval of the request the program change is written, tested and approved.

Errors will always occur in the input, processing and the programs. Controls must be established in every system to ensure that all errors are corrected and resubmitted promptly.

PART II

PROCESSING CONTROLS

Processing controls comprise by far the largest and most comprehensive group of new methods of controls offered by EDP. Not only is unprecendented accuracy and reliability attained in processing accounting data, but the impersonal nature of the computer permits transactions and file records to remain independent and assures that prescribed managerial policies will be carried out with a high degree of consistency. Processing controls are made up of checks built into the system by the manufacturer and checks capable of being incorporated into the computer's program. Processing controls are established to determine when data are lost or not processed and to check on the accuracy of arithmetic calculations.

The first group to be discussed relates to the "built-in" features, or what are sometimes referred to as "hardware", controls. Chapter 5 will discuss programmed or software controls.

Chapter 4

Built-in Controls

Manufacturers of electronic data processing equipment have built into their machines various error-checking techniques. Every machine on the market today has at least a few of these controls, therefore management must be aware of their scope and importance.

The most universal of all machine circuitry controls is the parity check. This particular check verifies each binary-coded character (a character being a letter of the alphabet, a number, or perhaps a special symbol, each of which is represented by a certain combination of zeros and ones). By adding another bit (a zero or one) to the binary code value when characters are being converted to machine code by some input medium, a condition is created whereby every character is made up of an even or odd number of ones. Computers designed to recognize an even parity count, for example, would process information containing only an even number of ones. The computer is designed to check this situation continuously at every point where information is transferred in its system. Any addition or loss of a bit distorts the character and will cause the machine to stop or correct itself by switching to an alternative program.

Some computers duplicate the more essential circuitry of their main arithmetic unit. This causes the calculations to be carried out twice to ensure accuracy.

In place of duplicate circiutry, some computers have a feature called dual arithmetic. Here the computer does not possess dual circuits, but auto-

matically performs every computation twice using the same circiutry. The results are then compared. (A few systems are capable of performing the second calculation with the complements of the true figures.)

Echos are often incorporated into the system at points where information is transferred. Here a feedback mechanism echos a character back from the point of transmission to its source. For example, when information is to be transferred from the computer to magnetic tape, the recording device senses what has been received and a signal is echoed back to the computer from the tape unit. This signal is then compared for accuracy.

The dual head is another method similar to echo checking, but is used in checking the transmission of recorded information. A reading device senses recorded information and transmits it instantly back to the source for comparison. Dual heads represent a much more effective check than the echo check, since the recorded information is checked, not just the electronic impulse.

The overflow control is designed to indicate whenever an arithmetic function causes the data to overflow the capacity of a counter or accumulator in the computer's arithmetic unit. This prevents the loss of significant digits during computation.

The sign control will indicate whenever an arithmetic function is per formed on an amount which does not carry a positive or negative designation.

When information is being written on reels of magnetic tape, old information is automatically erased. To assure that master files might not inadvertently be used on an output unit, a plastic ring is removed from the reverse side of the tape reel. Without this plastic ring no information can be written on the tape. This control is called the tape ring.

Although preventive maintenance is not part of the system, it is

included in this chapter because it does make use of some of the technical aspects of computer design. Normally a schedule is followed which allows a crew of engineers to devote at least one hour each day to preventive maintenance. Test problems are fed into the computer which check all of its components. A "high-low" voltage test is applied whereby the computer is tested to detect marginal functioning of its circuitry.

A special control terminal applies to on-line systems. It is a special piece of equipment that monitors the communications network, checks on the status of the terminals, and receives messages from the system concerning errors, invalid message codes, status of queue inventories, etc. Through the control terminal, the system can be shut down or started up, terminals can be added to or deleted from the network with this control terminal.

The control terminal operator is responsible for monitoring the system to see that it does not become overloaded.

In a multiprogrammed system (on-line), a number of different data elements will be in core storage at the same time. Because of the possibility of a programming or a machine error, an operational program could address protions of core storage outside the limits of its own coding, work areas, or other applicable areas. The result could be the alteration or modification of another program, the destruction of data or the creation of a series of endless loops. One technique to protect memory is the boundary register. This requires additional equipment in the form of an upper and lower boundary register. (The boundary registers are loaded with the upper and lower core storage addresses of the program when the program is loaded into the computer.) If the address portion of a program's instructions exceeds the boundaries indicated in the registers, an interrupt occurs, and control is passed to the supervisor program for appropriate action.

The computer system has automatic controls to prevent the equipment from attempting certain operations at the wrong time. "For example, there is an input/output interlock which prevents the computer from signalling an input or output device to perform an action while it is already performing another operation...A storage protection interlock is a hardware control used with a fairly advanced computer system that processes several programs concurrently. It prevents the computer from using a block of memory locations that are not assigned to the particular program."[1]

These represent the mechanical controls which have been built into the electronic data processing equipment by manufacturers. Management must be aware that these controls exist and are available to them in the various types of electronic data processing equipment.

FOOTNOTES

[1]Gordon B. Davis, Auditing & EDP, (New York, American Institute of Certified Public Accountants, 1968).

Chapter 5

Programmed Controls

Programmed controls represent checks capable of being incorporated into the compnter by means of coded instructions and control panel wiring. These controls are more sophisticated than built-in controls. Many of these controls are costly. Management must evaluate each technique in view of the safeguards received, the cost of writing the programs, the time it takes to run each of these checks, and risks taken if the controls are not taken.

A record consists of a group of characters which are normally considered together as a unit, such as the combination of numbers which make up a particular transaction or an account balance. The records are separated by blank spaces in the tape called interrecord gaps. These interrecord gaps are automatically created by the computer and indicate the end of one record and the beginning of another. The end of the file may be signaled by a special one-character record called a tape mark. The computer might be programmed to count the number of records it processes, and later this result can be compared with a predetermined total. Record counts are generally made a part of the information on every tape reel. Thus, file data can be transferred from one tape to another without fear of loss of records.

A sequence check is used in batch processing. It permits master records to be checked for ascending sequence while being read for processing. The records are in some kind of sequence, for example, by employee number or by stock number. Programmed checks to detect out-of-sequence,

duplicate and missing cards and records prevent a file from being processed in an incorrect order. These out-of-sequence, duplicate, and missing records can be listed for investigation.

A test may be used where limits are established to determine if the input record is more or less than the established limit. When processed data exceed these predetermined limits, the machine can be instructed to stop and special handling techniques can be designated by the on-line printer.

A proof figure can be used to check an important series of multiplications. An arbitrary figure, larger than any multiplier, is selected. Each multiplicand is multiplied once by its true multiplier and then again by the differences between the multiplier and the proof figure. Upon completion of a series of multiplications, the total of the products resulting from both multiplications is compared with the product of the total of the multiplicands and the proof figure. They should be equal.

Crossfootings have long been used by accountants in checking the accuract of individual postings. The computer can be programmed to perform this function.

Identification comparison enables data fields to be machine-checked against one another in order to prove the accuracy of matching, coding, balancing, and file record selection.

When only certain characters (such as zero or a blank) are acceptable in a data field, a valid character test may be programmed to ensure that no invalid characters are used.

A valid field composition test may be made to determine that a field that should contain only alphabetics or numerics actually does contain the proper composition of characters.

If a field on the input data should contain a specific number of digits, the program should test to determine that the field size is as specified.

If the sign of a field should always be negative or positive, a test may be used to ensure that the sign is correct.

To detect errors such as substitutions and transpositions, a check digit may be used. This test is most often used when data include identification numbers.

A tape label is a part of the record on each reel of magnetic tape. Certain identifying information can be written on the tape in the form of a lead record (external label). Desirable types of information which might be made a part of the tape label are: nature of the information on the tape, processing directions, frequency of use, earliest data the reel might be used as a new output tape (sometimes called the "purge" data), control totals, and name of the person responsible for the tape. The computer can be programmed to read this information before processing the tape. Internal header and trailer control labels may also be recorded on the tapes. The first (or header) record written on the tape gives the program identification number and other information. The last (or trailer) record contains a count of the number of other records on the tape.

The computer system might be programmed to monitor data fields at transfer points for blank or zero positions. The blank transmission test might be used to detect the loss of data and to prevent the destruction of existing records in file storage.

Failure to update a file may be sensed by comparing the contents of the file before and after each posting. This alteration test is similar to identification comparison.

The checkpoint or "rollback" and restart procedures permit the computer

to continue processing from the last checkpoint, rather than from the beginning of a run, in case of an error or an interruption in the program. Intermediate processing results, input-output records, as well as the contents or certain storage areas, are preserved at each program established checkpoint and are recorded internally in the computer. At the same time, if desired, accuracy of processing up to the checkpoint can also be established. In the event of an error, restart procedures permit the program to revert back to the last checkpoint, restores the main storage to its status at that checkpoint, and resumes processing.

After a programmed check signifies an error in reading or writing, a programmed error routine should cause the operation to be performed once again. If there is still an indication of an error, certain predetermined formal procedures for discovering what and where the error is should be made available to the operator outlining what action is to be taken.

A test may be programmed to ensure that all data fields necessary to process the transaction actually have the required data. This is called a missing data test.

An authorization test may be appropriate to determine whether the department originating the transaction is authorized to initiate the type of transaction.

Usually, only a relatively small number of valid transactions can be processed with a particular file. Therefore, a test may be used to ensure that only valid transactions are processed.

Error detection may be strengthened by considering data fields not only singly but also in combinations. Acceptable values for one field may depend upon the values of one or more additional fields. Therefore, a series or consistency tests may be necessary to test a combination of conditions.

Control totals can be used for testing the data processing within the system. Output control totals from the edit program should be used as input control totals for the update program and should balance to the output totals from the update program. Control totals developed during processing should be in a form which can be compared with the control totals for the data when they were key punched or first entered the computer system.

These are techniques that can be programmed into most computer systems. These controls and techniques are needed to insure the safety of the data put into the system. Management must be aware of the controls available to them to wisely make decisions about which techniques to program into the electronic data processing system.

PART III

ORGANIZATION AND ADMINISTRATIVE CONTROLS

The last two parts have discussed methods to assure that all valid data put into the system is processed accurately. These controls are necessary for every system, but they are useless unless some protection against natural disasters and people who unintentionally or intentionally destroy valueable information is available. This part will consider this type of protection. Chapter VI will discuss techniques to prevent disaster from environmental occurrences and Chapter VII will consider organizational controls as well as management's responsibility to see that all the controls are enforced.

Chapter 6

Equipment, File and Program Protection

Physical controls over files, programs, and the computer have been grossly neglected. Where other controls have been enforced marginally, physical controls have generally been abandoned.

Control measures for safeguarding the equipment and the computer records include physical safeguards, procedural controls, file retention plans and file reconstruction plans.

Physical safeguards are the measures employed to minimize the rish of environmental destruction of systems documentation, programs, data files, and the equipment. Physical safeguards include temperature controls, humidity controls, smoke detectors, fire detectors and exitinguishers, fireproof storage facilities, and security protection devices.

Probably the greatest exposure to loss arises from the possible loss of use of the equipment and of the records. Once a particular function is converted to EDP, the uninterrupted continuation of the operation becomes essential to the normal operation of the business. Minimizing or reducing losses in this area can be accomplished by duplicate records and stand-by equipment. The high cost of such stand-by equipment makes it unfeasible to purchase it. It is possible, however, to enter into a reciprocal arrangement with another user of compatible equipment for the exchange of facilities in event of an accident. "Back-up" arrangements with several users of similar equipment would be even better.

If the central processor does fail, the communications portion of the

total operating system can be transferred to the backup computer, the required peripherals can be switched over or files transferred, and a restart can be initiated. For this to be possible, the software system (the programs and related documents) must be able to accomodate different hardware environments, especially if the two hardware systems are not identical. The alternative is to initiate a restart from a different version of the software system. The difficulty with backup systems is to get someone with similar equipment to enter into the "backup" agreement.

A computer center should be located at a site where employees can get to work conveniently and safely. Within a building, the center should be located out of the main traffic flow, out of public view, and behind substantial walls.

To control access to the computer center, an electronically controlled double-door entry system could be installed. Once a person enters the first door into the buffer zone, the door locks behing him while he is subjected to an electronic search by concealed probes for magnets and other "illegals". If a magnet (or other illegals) is detected the system freezes the second door and automatically alerts the security guard. The second door can only be opened with a special badge-key issued to authorized employees. If the person doesn't have a badge, or if a wrong key is used, he is trapped in the buffer zone and has to call the guard via a voice communications system. The guard can view the buffer zone through a closed-circuit television camera.

Other steps in protecting computer security are:

1. Establishing guards at the entrance to computer centers and requiring identification badges to be worn by personnel having access to such areas.

2. More stringent security checks on personnel, particularly those who work on second and third shifts--even night cleaning crews.

3. Inspecting packages brought into computer centers.

4. Limiting areas to which visitors have access.

5. Where applicable, installing bullet proof glass and riot doors and reducing exposure of equipment and files to window walls.

Procedural controls are used to minimize the possibility of destruction through operator error. Some common procedural control methods include external tape and disk label, documented tape disk library procedures, off-premise file storage procedures to ensure against total destruction of essential records, preventive maintenance procedures to safeguard against equipment malfunctions and internal tape and disk labels.

A file retention plan provides the basis for file reconstruction in the event of file destruction. Retention of at least three processing periods for operating files (grandfather, father, son concept) is a normal standard. Transaction files necessary for recreating master files, must also be retained. Source documents, punched card files, tape files, deck files, and computer print-outs should be included in the over all retention plan.

The source documents on which an input file is based must be retained intact until such time as the file is proved and balanced with its controls. At this point, the data may be filed or otherwise disposed. However, both operating and legal requirements must be considered in developing a record retention schedule.

A data processing department should be able to reconstruct its destroyed records, using appropriate retention plans and safeguards. However, these reconstruction plans should be clearly documented to facilitate implementation by data processing personnel.

Source documents (unconverted records) and media (tapes, cards,etc.) should be evaluated for protection purposes. Records classified as "vital"

and "important" as opposed to "useful" and "nonessential" should be given special attention and kept in fire-resistent storage equipment. Duplication of records and storage in a safe place, preferably in a separate location, is the most desirable protection, particularly for those records that would be impossible to recreate if the originals were destroyed. Although the most desirable, duplication of a large quantity of records which are used frequently would be extremely expensive and time consuming and is not considered a practical answer to record protection. When revisions are made, copies of the revisions should be filed with the duplicate or back-up copy.

With punched card files the current master file should be copied periodically, and this copy should be stored at the outside location. The frequency of copying depends on the amount of update activity for that file and the retention of other files used to create a current master file. Each time a master file copy is created, the previous master deck and intervening revisions should be destroyed.

Backup support for tape files is usually accomplished by use of the son-father-grandfather concept. This concept is based on an operating procedure in which an updated master file is produced by reading the previous periodic master file, making changes according to the transactions being processed, and writing the new updated file.

To create a current master file in which the son-father-grandfather concept is used, the transactions used to update the master must also be retained; i.e., the transaction records for the previous processing cycle are required to update the "father" tape. Transaction records for two processing cycles are required to update the "grandfather" tape.

In the son-father-grandfather backup procedure, the old "grandfather"

tape may be scratched when a new current file (or "son") is created. Also, the transaction records processed with the "grandfather" tape can be released. Thus, if the respective transaction records are kept, two backup tapes are available at any time.

In most applications where disc files are used for storing master records, due to the processing characteristics of disc files, the old record is destroyed when an updating occurs. Therefore, unlike magnetic tape processing, disc file processing does not automatically produce a duplicate copy and the son-father-grandfather concept for file backing cannot be used.

Compared to tape, disc packs are expensive and do not readily lend themselves to daily duplication. In many cases, daily duplication of the disc pack may involve more time and expense than is justified by life retention requirements. As an alternative, except for the large data base files, a weekly disc duplication schedule, coupled with a plan for retaining intervening transactions, will provide adequate support. If this alternative is used, transactions must be retained until the related files have been balanced and until they are no longer required for purposws of support or other processing needs.

For the large data base files, the key to the time frame required to unload the disc for backup purposes would be the mean-time to repair. A weekly file dump is often not a sufficient process for backup purposes. The time frame required to reconstruct a large data base, with a high volume of activities, requires a different approach for data base integrity. For these files, maintenance of a journal of before and after images of the data base should be considered as an alternative to periodically dumped files. The costs of before and after images instead of periodic dumps should be considered.

A file may be retained by reproducing (dumping) it on another medium such as tape, cards, or paper. This procedure requires extra processing; also when the file is printed on paper, the information is not in machine-readable form and must be repunched before it can be used to recreate a file. Such a process is very inefficient but should be used if no other form of backup is available.

A procedural control for "on-line" or "real-time" systems is a procedure which permits only one transaction to update a file at a time. In the IBM system software package this is referred to as "exclusive control".

"Exclusive control" can be achieved by requiring each transaction to "request" permission of the supervisory program to update a file. If the file is available, the supervisory program grants the request and the transaction updates it. During this time no other transaction is permitted access to this file.

The prevention of unauthorized access to stored data can generally be accomplished by the use of lockwords, authority lists, and dedicated communication lines. Lockwords, sometimes referred to as "keywords" or "passwords", consist of several characters in a data file which the input transaction or inquiry must match in order to gain access to the file. The use of this device to control file references may be further refined by supplying several lockwords. For instance, one set of characters may permit the file to be retrieved for reading purposes only (read-protect), and still another set may permit both reading and writing.

When using lockwords, consideration should be given to the type of terminal used. If the lockword appears on each document printed by the terminal, it may defeat its own purpose since it becomes relatively easy to compromise it. There are devices available from which the lockword can be

entered into the system in a non-print mode. This type of terminal should be used where feasible.

Authority lists are another form of protection. In this instance, the lockword is used to identify the person transmitting from the remote location. After the initial identification has been established, reference is made to an authority list which indicates which type of data the sender is authorized to receive. As with lockwords, the authority list may classify references to the files as read only or both read and write. The extent to which these controls are used will depend on the type of system and the nature of the stored data.

Another way to prevent unauthorized use of data is to have controlling pathways. This is where the data base of a computer's memory is structured like a tree. The system makes a security check on the user at each junction of a branch to the tree trunk. User A, for example, may be authorized for access to only a certain portion of the computer's memory or files of information. When he arrives at the junction, his identity will be checked and he will be allowed to examine the data leafs on that branch. If he attampts access to the computer's files at any other junction, his identity will not match and he will be denied entry.

Another idea is the "rings of protections." The data base is structured, in addition to a tree or pyramid structure, in rings or concentric circles. A user is allowed to enter a ring only at a carefully defined point, and once he enters the ring, the way the information is processed and handles is completely beyond his control.

When lockwords and authority lists are not used, terminals may be identified by means of dedicated communication lines. This generally implies the use of only one terminal on the line. Where terminals are attached to

a party line or a similar network, answer back would be used in lieu of a dedicated communication line. With answer back, a signal is sent to the terminal, and the latter responds within a prescribed amount of time with its code identification. Because this system can be compromised, it is not recommended where the security of stored data is of major importance.

To prevent an unauthorized individual from transmitting data to the processor in an attempt to decode the lockword and gain access to the system, a monitoring routine could be established which would count the number of unsuccessful attempts to enter the system and after a certain number had been reached, say three times in succession, a message might be printed out at the data station with instructions to call the downline station for an explanation.

One of the characteristics of a real time system is that it must operate without stopping for fixed periods of time. If there is some malfunction or programming error that occurs while the system is operating, the system should keep operating if there is some way of circumventing the trouble. To accomplish this objective, it is necessary to build into the system some way of detecting and isolating error conditions so that appropriate action can be taken.

Diagnostic programs are a tool used to test computers, isolate component malfunctions, and improve overall computer system operations. For purpose of illustration, the following is an example of how these programs might work:

> Consider a real time system communicating with a number of remote terminals. Suddenly a terminal breaks down. When this happens, a diagnostic program checks the communication network and establishes that there is a problem. Another diagnostic program checks each line until the down terminal is isolated. Once the error has been isolated, control is returned to the supervisory program, which might close down this line until repairs are made and route all interim messages to an adjoining terminal for manual handling."[1]

To detect that errors are happening and to isolate these errors, one of six actions can be taken:

1. Re-execute the faulty instruction and continue processing.
2. Restart the program in question.
3. Transfer to an exception routine characteristic of the program in question.
4. Initiate switchover.
5. Initiate closedown.
6. Halt.

The first three of these have been satisfactorily tested in the traditional batch processing systems, and similar procedures can be incorporated into real time systems. The last three alternatives are unique problems and require careful consideration if the system is to provide for all contingencies.

Failures that can cause a system to switch computers or closedown a part of the system are generally due to hardware malfunctions. When a system is able to switch its operation from one computer to another, as is possible in a duplexed system, without changing its method of processing data, we say a "switchover" has occurred. On the other hand, if an equipment malfunction occurs in the system which requires the system to close down some part of the operation and modify its method of processing data to circumvent the error, we say it is functioning in a "fallback" mode. Whenever either of these conditions arises it ia necessary to provide procedures to ensure that they are effeciently handled.

Switchover, as stated previously, assumes the use of duplex computers so that if the operating computer breaks down its supporting unit will take over processing. When the change from one unit to another takes place, whether

it is automatic or manual, the machine operator should be informed via the console or printer what action he is required to take, if any, and the reason why the change was made. For an automatic switchover to take place, the on line computer should initiate action. However, if the malfunction is serious, this may not always be possible. To ensure that a changeover is effected when such a malfunction occurs, the standby computer should periodically check its counterpart. If it detects a malfunction, it should initiate the switchover. Whenever this transition takes place, a message notifying terminal operators of this fact should be sent down line.

During the transition it is vitally important that transactions not be lost. These controls have been discussed in Chapter 1.

"Fall back" or "graceful degradation", as it is sometimes called, occurs in a non-duplexed system when a part of the equipment configuration breaks down but the loss of the particular piece is not serious enough to shut down the entire system. When this happens, the machine operator should be informed by the control program as to the current status of the system and what action he should take. In some instances terminal operators should also be informed. Procedures should be abailable tocadvise supervisory personnel what clerical action is necessary to support the system until it recovers and, finally, what action is necessary to restore the system to the condition that existed before the fallback occurred.

The results may be catastrophic when a real time system halts. If the halt is due to a complete breakdown of a major component, the only thing to do is repair it as rapidly as possible. Procedures should be available for supervisors so that they may take necessary emergency action and guide clerical personnel in work which must be done while the system is down and initially after it recovers.

It is imperative that restart procedures be incorporated in the system. The restart is based on a complete checkpoint record (checkpoint procedures are discussed in Chapter 5), written on a peripheral device such as a disk file. The checkpoint record, provision for which should be incorporated in the system, is a complete record of all messages, counters, logs, and status indicators in the system at that time. When a restart is necessary, the checkpoint record is used to restore the system to its condition at the time the checkpoint record was written. Each terminal is advised of the restart and the number of the last message properly received from the terminal at the time of the checkpoint. Subsequent messages are retransmitted, and the system is again operational.

If the halt occurs because of a system overload the problem is not as serious. System overloads can occur when a number of messages are read into core and subsequently it is discovered that there are not enough available core blocks to complete all the work the computer has started. This problem can occur in a multiprogrammed system using random input. There must be some emergency procedures in the system to handle this dilemma.

It is possible to prevent this from happening, except in rare instances, by anticipating when the level of core blocks available for processing data in the computer is reaching a danger point. When this level has been reached, the computer should shut down and refuse to accept any more input. This means the computer must be able to control the volume to input during peak periods. This control is exercised in a system utilizing "polling" techniques by not "polling" transmitting locations until the overload is ended. Another method that may be used is for the processor to send a signal either requesting the operator to reenter the message into the system or locking the terminal pending further notice from the computer.

If the overload does occur, however, the system should be able to handle the problem by first determing the application programs temporarily in core which are not currently being used and making their applicable blocks available for the further processing of data. If this doesn't solve the problem, the system may have to destroy messages in the system, preferably on a last-in basis, and request the applicable terminals to repeat the messages.

There are many fire protection devices available. The best are those that detect the fire and give the alarm earliest.

Computer centers should be constructed of fire resistant materials. The floor is generally raised 18 inches to hide the cables. The raised flooring also allows smoke detectors underfloor as well as ceiling smoke detectors. The underfloor zones can be baffled to inhibit the spread of fire.

The center can be divided into zones and each zone served be an overhead and an underfloor detector. Control panels located in the computer area and another in some other part of the building can monitor the fire detectors. When a fire occurs, the control panels will immediately locate the fire.

When a fire occurs, personnel should manually shut down the air supply to the room and the computer equipment and undertake initial firefighting efforts using manual equipment.

An on-and-off recycling pre-action sprinkler system has the capability of continued on-and-off cycling while controlling the fire and of shutting off the flow of water automatically when the fire is extinguished. This will reduce water damage to the highly sensitive equipment.

The National Fire Protection Association has made extensive recommendations concerning computer installations. Some of these recommendations are:

1. Availability of carbon dioxide extinguishers.

2. Storage of vital records in storage cabinets having a class C rating (one hour at 1700 Fahrenheit).

3. Personnel trained in fire control procedures.

A breakdown in the processing center jeapordizes the entire business operation. Management should be aware of the implications resulting from the possible damage to or destruction of all records and equipment utilized in the EDP operation. Management should also be aware of the various types of insurance available to provide some protection to the business in case of disaster. The types of insurance available has been categorized according to types. A discussion of the varous types of insurance available to computer centers is included in Appendix B.

To be used effectively, a computer requires a controlled physical environment. It begins with a careful layout of the computer room. Most hardware manufacturers furnish clear overlays which can be used to position the planned view of equipment for floor and arrangement planning. These overlays of equipment can help management determine the most efficient layout of the equipment. Dust, humidity and temperature requirements for a data center have become less stringent in the last few years but they are still important considerations. They must be controlled to ensure that the atmosphere is maintained at the desired level for effective operation of the equipment. In effective atmosphere controls may lead to equipment failure and loss of records. (For more specific detail see Appendix A.)

As computers become more and more important to the success of a business, management must employ all the controls and precautions necessary to protect the computer equipment and records from disasters--both natural and man-made.

FOOTNOTES

[1]Robert F. Moloney, "New Generation EDP Control Considerations," (March-April 1968):19-20.

Chapter 7

Organizational Controls

Good computer control requires something more than machine reliability. It requires specific measures that are imposed on the system to control the actions of people. This chapter will discuss the organizational controls that increase security and reliability.

The computer center should be a separate service center processing data for user departments. Entries should not originate there nor should proof totals be agreed there.

In large scale systems, the security of the systems should be under the control of a security officer, and under the data base administrator in medium or small scale systems. In multiple plant locations there may be more than one security officer, and each should have a designated sphere of authority with control over modification of pass words and control techniques within his sphere. The security officer should be responsible for monitoring the system for attempted security breeches, for quickly following up on security violations, and for removing a terminal or terminals from the network or taking other action to protect the data from unauthorized access.

Some companies have organized separate control groups to control all input and output from the computer. This group receives data and control figures from the user departments and agrees resultant runs and reports to these control figures. (In large companies, the internal auditor is part of the control system.)

This control group (or control desk in smaller departments) should be part of the data processing department for three reasons:

1. A single communication point with the data processing department is provided for all departments.

2. The control desk can usually better adapt to the strict scheduling requirements of the EDP unit if it is part of the data processing department.

3. The procedure normally provides better communication between control personnel and systems designers.

The control desk directs the flow of data to and from the computer and monitors the system controls during the actual processing of the data. A primary function of the control desk is comparison of batch or control totals.

There should be a separation of duties between programmers and computer operators. Internal control can be strengthened by the proper separation of the duties of the programmers, who have the detailed knowledge of how the programs operate, from those of the operators who may have the opportunity to manipulate the programs. Operators should be rotated between shifts and jobs. Everyone in the department should be required to take vacations. (See exhibit C for detailed description of job separation.)

Individual responsibilities should be clearly defined for all data processing functions including top management, data processing activities, computer operations, data preparation, and data control. These job descriptions should be written up formally. The manual prepared should establish relationships of responsibilities, as well as define work assignments.

Standards of performance should be established to measure individual accomplishment. Adequate training programs should be instituted to ensure

the level of competence necessary to achieve desired results.

Documentation consists of the written information necessary for communicating the essential elements of data processing systems and programs. Data processing documentation can serve to provide material for supervisory review, system and program revision, inquiry response, new personnel instruction, and internal control evaluation.

Documentation in data processing operations provides a source of knowledge regarding the installation's standards of performance. It should be prepared, reviewed, authorized and updated as required.

Documentation standards should cover coding conventions, decision table conventions, flow-charting conventions, provisions for modification, and a glossary of terms. In addition, details as to recovery and restart procedures and end-of-job procedures as well as message codes should be included.

An effective documentation plan, as illustrated in exhibit on page 54, should include at least the following:

-An installation standards manual describing the procedures for designing systems, writing programs, and operating computer equipment

-System documentation providing an overview of the total application, and tying together the individual computer runs within a distinct system. Input data sources and formats, output data formats, tape and disk record formats, system logic, and program test data may be included as system logic, and program test data may be included as system documentation.

-Program run books representing the complete documentation of an operating program. The programmer documents the logic followed by the program, as well as other pertinent details such as input/output

descriptions, operator instructions, program coding, test data description, file contents, and flow charts.

-Operator run manuals explaining how a particular processing job is to be performed, and the prescribed actions to be taken by the computer operator.

-Key punch manuals describing the pertinent card fields for each source document and keypunch machine settings and adjustments.

-Clerical procedures manuals explaining the step-by-step preparation of various computer input forms, the manner in which output is settled, and other various control points for data flowing through the system.

-Descriptions of special treatment required for exceptions.

-List of programs required by the system and a description of the functions performed by the program and a general description of how the program accomplishes them, with particular attention to features of the program or logic that would otherwise tend to be obscure.

-Constraint codes and tables.

-Processing controls and data validation considerations described.

-File control procedures should be defined clearly.

-Audit management trails should be specified.

-Conversion procedures and schedule listed.

Control reports should be printed at various stages during processing. The reports are required for controlling the system and for constructing the audit trail of the data processed. A control report should be printed by each program in the system. The reports should include the following:

1. Program name and for number and data of run.
2. Labels of input and output tapes.
3. Control totals of data processed.

4. Error messages, which also may be printed on a separate error listing.

5. Results of balancing (the comparison of control totals) if done by the computer.

For on-line systems, a console log records an audit trail of internal events, supplies operating instructions, and allows the operator to communicate with the computer. All messages displayed by the console should be date- and time-stamped. The partition and operation issuing the message should be identified. Messages should be standarized and, above all, kept to a minimum. Most of the messages should be software-generated and in the form of operator directives. Operator input through the console should be stringently edited and standardized. All operator messages should receive a response even if rejected.

An on-line system should also have a history log. Its contents include:

-All input communication messages.

-All output communication messages.

-Desk images for recovery.

-Hardware failure messages, both central and remote.

-Beginning and end of program indicators.

-Communication startup and shutdown detail.

-Message header inconsistencies.

-Communication status changes.

-All unusual occurrences, such as recovery or program failures.

The history log should be maintained on a low cost medium, usually tape. It serves primarily as backup, but since it is a machine readable audit trail, it can also provide the basis for mechanized analysis of systems effectiveness. The history log can be used to identify sporadic line terminal,

or peripheral device problems before a complete breakdown occurs, to detect attempts to break security, and to perform volume analysis.

It is essential to maintain control over commands to the communication software system. Most communication systems are shut down at least once a day to permit basic housekeeping maintenance and backup procedures. Shutdown and startup should be thoroughly documented on the console and control terminal including time, operator and any unusual conditions. Where it is not possible to do a normal shutdown for hardware or remote terminal reasons, an emergency shutdown should be available. Since restarts after an emergency shutdown require recovery information, the software must prevent a normal startup from being accidently initiated after an emergency shutdown. In such circumstances a recovery startup should be made, for a normal startup would result in the loss of any messages remaining from the previous day and probably preclude any possibility of their recovery.

Since it is a necessary software feature to have the ability to make status changes to the communications software system while it is operational, the status changes should be well controlled. Requests for such changes should be permitted from authorized locations only, such as the logging terminal. The requests should be stringently edited, the new status documented in detail and a regular reminder of status changes sent to the control terminal. In this way, no status changes can be made by unauthorized personnel or by accident.

Top management has the overall responsibility for data processing. Millions of dollars of control features can be installed in the system with little or no effectiveness if management doesn't see that the controls are enforced.

Management's total responsiblility consists of authorization of major

systems additions or changes, post-installations review of actual cost and effectiveness of systems projects, review of organization and control practices of the data processing function, and monitoring of performance.

Top management responsibility for authorizing major system work means that each such major addition or change must be presented to management as a proposal to be evaluated in terms of its cost and the benefits to be derived from it. Management, then, has a responsibility to be aware of the capabilities of computers so they can make intelligent decisions.

Once the system is installed, management should evaluate the project and any deviations from the estimate given in the project proposal. This could save the business money by preventing the same mistake from happening twice.

Top management is also responsible for employing competent, adequately trained data processing management personnel. Incompetant personnel can be one of the most expensive aspects of a data processing department.

As you can see, management must become familiar with EDP in order to be able to control it. It is essential that management understand EDP before initiating the system. Management must tailor controls to meet the requirements of the particular company's need. They must consider the economic balance between the value of controls and their costs. These controls must be designed at the time the EDP system is being established. The price for failure, in addition to the errors and system stoppage is considerable redesign and reprogramming expenses. Failure to implement and enforce these controls could mean economic disaster to the business.

APPENDIX A

COMPUTER FACILITIES

An often neglected area of computer management involves the physical location for the machine. Along with the decision to acquire computer hardware is the requirement for a place for the equipment to operate. Each computer generation has become progressively less of a problem in terms of facilities. Size has been reduced, heat loads have dropped because of transistors and semiconductors, and the equipment is less sensitive to environmental conditions. Nevertheless, computers do require special treatment.

Heating, ventilating, and air conditioning requirements are not as demanding as they were a few years ago. Since the data center equipment is heat generating in itself, heat sufficient for personal comfort will also be quite sufficient for the equipemnt. The allowable humidity range is broad, usually between 10 and 80 percent.

A primary factor in both heating and cooling loads is the heat gain or heat loss through the environmental structure. This is determined by the following formula:

$$q = \frac{AKm(t_1 - t_2)}{x} \quad \text{Btu per hour}$$

where q=total heat loss or gain, A=transfer area in square feet, (t_1-t_2)= inside/outside temperature difference (^{O}F), and X=wall thickness in feet.

Typical Km values (perfect): Wallboard--0.3, wood--0.1, glass--0.5, brick--0.5, concrete--0.8, steel--26.0, aluminum--118.0.

Air is the basic medium for heat exchange in a data center. The air

flow required is $Q=\frac{q}{1.08(t_1-t_2)}$ where Q= heated air (CFM), q=heat load (But/hr), and (t_1-t_2)=difference between heat source and room temperature. In addition to heat transfer, about 30 CFM of air per occupant is recommended for ventilation.

This adds two heat loads, the sensible heat load is (based strictly on temperature change) q_s-1.08 $Q(T_0-T_1)$ where q_s=sensible heat load, Q=CF ventilation air, and (T_0-T_1)=temperature difference. There is also an additional heat load resulting from the introduction of moisture from the outside.

In calculating air conditioning loads, the heat transmission through wall surfaces and the introduction of heat gain from the outside air is calculated using the same formulas. An additional heat gain to be considered in air conditioning is the heat gain from equipment and lights. The following formula applies:

Heat gain q=3.42 w

where q=Btu/hr, and w-watts of electricity used.

People should also be considered as a heat gain. There are two sources: the sensible heat gain in Btu's and the gain due to the moisture passing from the person to the air, called latent heat gain. A reasonable average per person would be a total of 500 Btu's per hour.

The cooling load is the sum of the heat transfer, people heat load, appliance, and equipment heat loads. The load in air conditioning tons equals the Btu load per hour divided by 12,000. (The standard definition of a ton refrigeration is the amount of cooling that could be done by a ton of ice melting in 24 hours, which is 12,000 Btu's per hour as an accepted standard.)

The air handling units for both the heating and air conditioning system may be included with the unit or may be in a series with it. These are

basically enclosed fans. The air must be filtered. For optimum dust control, the data center should include positive air cleaning equipment.

The basic power requirements for the data center are the sum of the requirements for the individual pieces of equipment. Building codes will generally require the running of power cable within a steel or aluminum conduit. It is good practice to keep the power circiutry for the computer equipment separate from other power users extraneous to the data center.

In the average installation, there will be two to four levels of protection against voltage overloads. The first of these would beat the power transformation station where major disconnects and circiut breakers are installed by the utility company. The final protection would be at the equipment, where it is often customary to install a maximum overload fuse or a circuit breaker device. The systems servicing the computer center, should have maximum lightening protection and should meet the more stringent range of code requirements in terms of protection.

A data center should be well lighted during normal operations. A light level between 60 and 100 foot candles is recommended. Foot candles are calculated by the following formula: $(Ft\text{-}c)=\frac{LUM}{A}$ foot candles where L=lumens furnished, U=utilization factor, M=maintenance factor, and A=room area in square feet.

APPENDIX B

INSURANCE COVERAGE

1. Records and Equipment.

A. Property insurance (loss or damage to the system, including equipment and records)--In general, there are four existing forms designed to provide coverage on personal property such as EDP system property including supplies, equipment, and records. Since these coverages have exclusions and limitations, EDP system users should determine what coverages are available and to what extent coverage is provided.

(1) Standard Fire Contents Form. This form covers property of the insured, or property of others for which he is liable, of others for which he is liable, on an actual cash value basis. Coverage may be afforded against the perils of fire, extended coverage, vandalism, and sprinkler leakage. Records, including source documents and media, constitute "contents" under the standard form; however the extent of coverage is questionable. The advantage of this form is that it is available for covering all contents in an office and not just the EDP system. The principal disadvantage is that this is a specified peril form, and the exposure to damage and the costly nature of EDP equipment suggest separate, broader coverage.

(2) Office Contents Special Form. This form is designed to provide All Risk coverage to "Business Personal Property of the insured usual to the office occupancy--" and to "similar property of others held by the insured and for which the insured is liable." There are limitations on the amount of insurance afforded; mandatory co-insurance is required as are

deductibles for specific exposures. As in the Standard Fire Contents Form, the event to which this form covers items that are both media and integral part of the equipment (such as magnetic disks) is questionable and subject to interpretation. There are certain exclusions, such as mysterious disappearance and fraudulent or dishonest acts of the insured or his employees, incorporated in the form. The form itself should be reviewed to determine all exclusions applicable. This form is excellent for providing insurance on an office containing an EDP system and has the advantage of covering all contents, not just the EDP system. As to the coverage on records and media, while it is all risk, it contains a "books of accounts" limitation (usually a dollar limit of $500 is paid for reporducing books of accounts, card index systems, etc.), coinsurance is mandatory, and it is not the most satisfactory form for insuring valuable records and media.

(3) Valuable Papers and Records Form. This form is very broad and does not exclude earthquake, disappearnace, dishonesty of employees, and other items excluded in the other forms. It does not contain a coinsurance clause but does require that records that cannot be replaced must be specifically insured at an agreed value. When this is not done, loss is limited to the "actual cash value" of damaged or destroyed records or the cost to replace. The Valuable Papers and Records policy may be subject to a requirement that the papers and records be kept in certain protective devices when not in use.

(4) Accounts Receivable Form. This is another form of valuable record insurance. The primary coverage is against an indirect loss, since it covers the inability of the insured to collect money due him as a result of the destruction of his accounts receivable records.

(5) Special Data Processing Policy--Equipment. This is a special policy offered by a few insurance companies designed to provide broad all

extra expense incurred to continue the normal operation of the business immediately following damage to or destruction of (described) buildings or contents by a peril insured against. This would include the EDP system, but a special exclusion eliminates the reconstruction of records. This limitation makes this coverage unsatisfactory for loss to records and media.

C. Data Processing Extra Expense Form. This is an all risk form designed for insuring data processing systems. It is probably the only extra expense form that will definitely provide extra expense coverage arising from the destruction of EDP media.

The tremendous investment made in EDP systems by business organizations and the extent to which these EDP systems by business organizations and the extent to which these EDP systems are integrated in the organizational operations makes it mandatory that managers responsible for the EDP activities be aware of the implications resulting from damage to or destruction of the systems.

As a part of their control function, managers should determine the extent of loss that could develop from damage to or destruction of equipment and records. As a means of reducing the risk and exposure, certain protective measures can be implemented. These include: keeping vital records in fire-proof safes when not in use; duplicating records where practicable; developing a "disaster plan"; and working out "back-up" arrangements with other users of similar equipment.

While not reducing the risk or exposure, insurance coverages are available for EDP equipment and records. The standard forms afford coverage for EDP equipment, though not as broad as that available under special forms. None of the "Standard" forms provides adequate coverage for reconstruction of information contained on records and media. The special data processing forms do provide a more complete coverage for insuring EDP media and for

the extra expense arising out of damage to or destruction of the media.

A prudent manager will recognize his risk exposure, take appropriate measures to minimize these risks, and in conjunction with whoever is charged with record protection, will obtain applicable insurance coverages to indemnify his organization in case of loss.[1]

FOOTNOTES

[1]Joseph Verba, "Protecting Your EDP Investment," Management Services, (September-October 1970):39-40.

EXHIBIT A

SUMMARY OF COVERAGE PROVIDED BY DIFFERENT POLICIES FOR DATA PROCESSING FIRE RISKS

TYPE OF RISK	FIRE COVERAGE	VALUABLE PAPERS COVERAGE	DATA PROCESSING COVERAGE
Damage and/or loss of equipment whether leased or owned	Cost of equipment	None	Cost of equipment
Loss or destruction of programs(software)	Cost of materials(cards and tapes) and labor (keypunching). No coverage for costs of programming or systems design.	Extent of coverage in doubt. May exclude recovery for loss of data stored on disks, tapes, or drums. However, may cover loss of software in punched card form.	Cost of reconstruction under critical conditions provided that remore storag is employed for key files and documentation.
Loss or destruction of data when reconstruction will be costly, time consuming and difficult.	Cost of materials on which data was recorded.	Extent of coverage in doubt.	Cost of reconstruction under critical conditions, provided that remote storage is used.
Extraordinary expenses incurred to return to normal operation.	None	Extent of coverage in doubt.	Covered.
Loss sustained by interruption of business.	None	None	Covered.

Gordon B. Davis, Auditing & EDP, American Institute of Certified Public Accountants, 1968,102.

EXHIBIT B

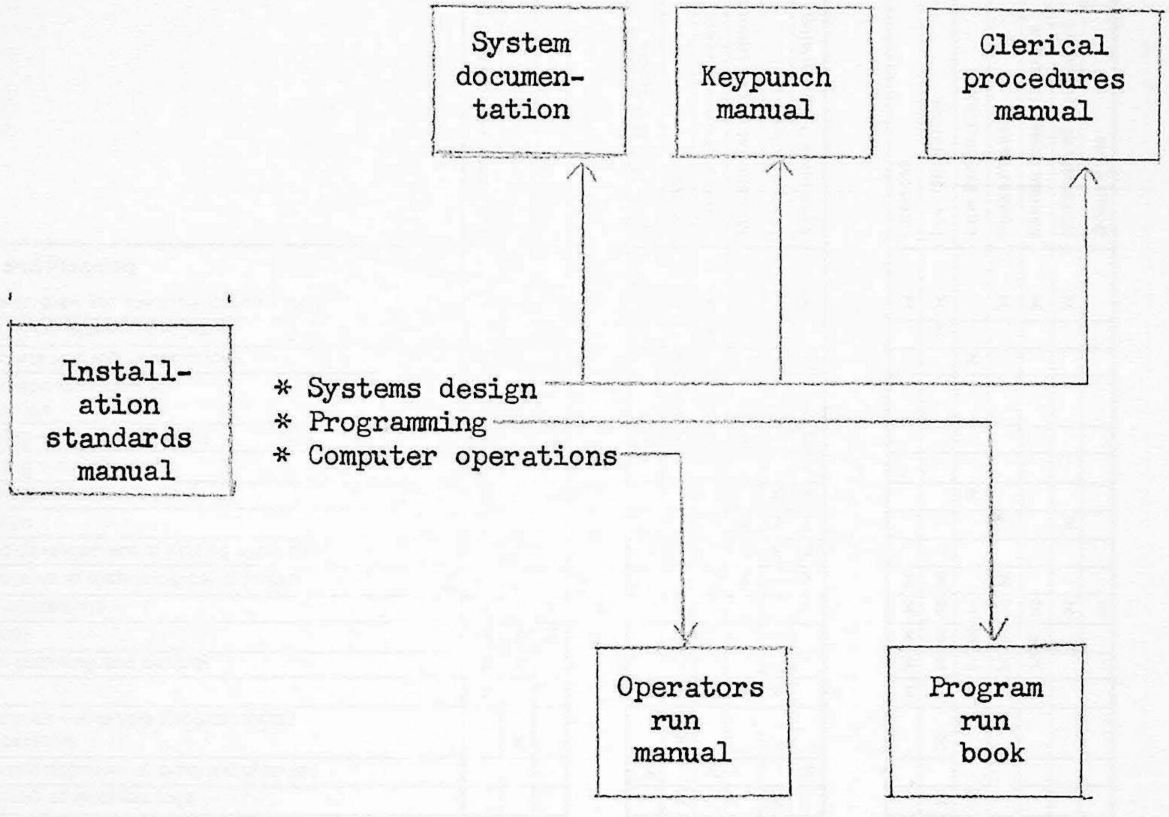
DATA PROCESSING DUTIES TO BE SEPARATED

Position	Description
Systems analyst	Analyzes requirements for information. Evaulates existing system and designs new or improved data processing procedures. Documents the system and prepares specifications which guide the programmer.
Programmer	Flowcharts the logic of each computer program. Codes the logic in the computer program language. Prepares program documentation.
Computer operator	Operates the computer according to the operating procedures for the installation and the detailed prodecures for each program found in the applicable program run book.
Keypunch operator	Prepares data for computer processing by keypunching cards according to instructions in the keypunch manual.
Data preparation and control	Prepares source documents for keypunching and monitors the accuracy of computer processing based on the procedures in the clerical procedures manual.

Harry R. Reider,"Safeguarding Computer Records," Management Controls, (October 1972) 246.

EXHIBIT C

AN EFFECTICE DOCUMENTATION PLAN



Harry R. Reider, "Safeguarding Computer Records," Management Controls, (October 1972) 246.

EXHIBIT D

RECOGNITION OF EDP OPERATIONAL PROBLEMS

(The following grid has been designed to aid businesses in identifying operational difficulties in their EDP systems.)

Absence of the following techniques leads to adverse results:

Adverse Results

	Effect on Employees			Effect on Systems						Effect on Equipment							Other Effects			
	Idleness/Unnecessary Staff	Constant Overtime	Turnover	Multitude of Projects	Delays	Limited Savings/Excessive Costs	Managerial Needs Unmet	Inaccuracies	Excessive Programming	Idleness	Low Utilization	Low Production	Peaks/Valleys	Excess Usage Charges	Multitude of Equipment	Down Time	Risk of Fraud or Vandalism	Wastage of Supplies	High Purchasing Costs	Costly Reconstruction
Organization and Planning																				
Long-term master plan for systems development	X	X	X	X		X			X	X	X		X	X	X					
Executive support for systems program			X			X	X				X									
Organization charts and job descriptions	X	X	X		X							X					X			
Assignment of responsibilities for:																				
Systems design	X			X	X	X	X		X								X			
Programming – systems changes	X			X	X	X	X		X								X			
Programming – maintenance	X		X		X				X								X			
Programming – standards	X		X					X	X			X								
Forms design							X	X	X						X			X		
Design and development of coding systems							X	X	X											
Keeping abreast of technological changes							X		X	X	X		X							
Computer operations	X	X	X		X					X	X	X	X	X	X	X				
Keypunching	X	X	X							X	X	X	X							
Production planning and control	X	X								X	X	X	X	X						
Library	X				X			X		X							X			
Separation of duties – Analysts-Programmers/ Computer Operators		X			X						X						X			
Authorizations and approval of program changes				X		X			X								X			
Supervisory review of machine logs					X			X			X	X					X			
Systems Analysis and Programming																				
Project controls relating to:																				
Project objectives				X	X	X	X													
Project benefits						X	X													
Project costs						X														
Testing and/or acceptance							X	X		X							X			
Supervisory review and approval							X	X									X			
Progress review	X		X			X														
Post completion evaluation						X														
Documentation of study and conclusions							X													X
Project priority assignments and backlog controls	X	X	X	X	X															
Participation in projects by users	X				X	X		X									X			
Participation of internal auditors:																				
Planning and development of project proposals							X										X			
Pre-installation review emphasizing internal controls					X			X		X							X			
Review of project documentation									X											X
Review of test documentation (for adequacy and control purposes)							X	X									X			

EXHIBIT D (CONTINUED)

RECOGNITION OF EDP OPERATIONAL PROBLEMS

Absence of the following techniques leads to adverse results:	Adverse Results																					
	Effect on Employees			Effect on Systems						Effect on Equipment								Other Effects			
	Idleness/Unnecessary Staff	Constant Overtime	Turnover	Multitude of Projects	Delays	Limited Savings/Excessive Costs	Managerial Needs Unmet	Inaccuracies	Excessive Programming	Idleness	Low Utilization	Low Production	Peaks/Valleys	Excess Usage Charges	Multitude of Equipment	Down Time	Risk of Fraud or Vandalism	Wastage of Supplies	High Purchasing Costs	Costly Reconstruction
Current Operations																				
Completeness/security of documentation for existing applications:																				
Systems descriptions		X					X	X	X											X
Run manual, including source listing or deck	X										X	X					X			X
Operator instructions	X										X	X					X			
Test data, current and available		X						X	X								X			
Record of changes to programs		X							X								X			
Use of programmed data controls where opportune								X				X					X			X
Use of multi-programming, as appropriate to improve computer utilization		X									X									
Use of outside services to level peak loads	X	X	X		X								X							
Preventive maintenance, and use of related outside services as appropriate	X				X											X				X
Scheduling of computer and of peripheral equipment	X	X			X					X	X		X	X			X			
Planning and supervisory authorization of overtime		X															X			
Consideration of high-speed input/output devices	X	X									X	X								
Consideration of sectional core											X									
Time and activity reporting system	X						X										X			
Consideration of key-to-tape and/or key-to-disk			X					X				X								
Consideration of source data automation	X							X			X						X	X		
Preparation of periodic summary reports:																				
Computer utilization						X					X	X					X			
Preventive maintenance																X				
Down time						X										X				
Rerun time						X		X				X						X		
Production time						X						X					X			
Time charges to users				X	X	X	X										X			
Periodic review of equipment utilization		X				X				X	X			X						
Periodic studies of equipment "balance"						X				X	X			X						
Periodic study to consolidate or decentralize data processing functions						X				X	X									
Use of electronic switching, as appropriate in a network of computers					X						X									
Security																				
File protection in terms of the storage of copies in loss-proof vaults	X									X							X			X
File reconstruction capabilities	X									X							X			X
Restrictions on access to necessary personnel																X	X			X

EXHIBIT D (CONTINUED)

RECOGNITION OF EDP OPERATIONAL PROBLEMS

Absence of the following techniques leads to adverse results:	Adverse Results																			
	Effect on Employees			Effect on Systems						Effect on Equipment							Other Effects			
	Idleness/Unnecessary Staff	Constant Overtime	Turnover	Multitude of Projects	Delays	Limited Savings/Excessive Costs	Managerial Needs Unmet	Inaccuracies	Excessive Programming	Idleness	Low Utilization	Low Production	Peaks/Valleys	Excess Usage Charges	Multitude of Equipment	Down Time	Risk of Fraud or Vandalism	Wastage of Supplies	High Purchasing Costs	Costly Reconstruction
Guards, lockable doors, and other protection devices																X	X			X
Terminal and access codes								X									X			
"Instant" terminations of data processing employees																X	X			X
Emergency power backup	X									X							X			
Emergency computer installation backup	X				X												X			
Buying of Computer Resources																				
Observance of sound procurement practices relating to specification of needs, shopping of market, preparation of complete purchase orders, etc.							X					X			X	X	X		X	
Evaluations of financial and performance capabilities of potential vendors																X			X	
Evaluation of vendor contracts by legal department, as appropriate																X			X	
Periodic lease or buy studies																			X	
Periodic studies of independent peripherals versus main-frame manufacturer												X							X	
Miscellaneous																				
Sale of waste paper and cards																		X		
Program for cleaning and testing and/or replacing magnetic tape					X			X		X										
Controls over computer time sold to outsiders													X				X			

Chart on EDP Operational Improvement Opportunities

Rapid advances in computer technology can result in systems that are vulnerable to operational inefficiencies. The chart on EDP operational improvement opportunities has been designed to alert businesses to various techniques that have shown their worth in actual experience. However, the chart should not be used without carefully thought-out fact-finding and evaluation procedures.

"Chart on Recognizing EDP Operational Problems," Lybrand Newsletter, (September 1972).

BIBLIOGRAPHY

BOOKS

Bohl, Marilyn. Information Processing. Chicago: Science Research Associates, Inc., 1971.

Chapin, Ned. An Introduction to Automatic Computers. New York: Princeton: D. Van Nostrand Company Inc., 1963.

Daniels, Alan and Yeates, Donald. ed. Systems Analysis. Palo Alto: Science Research Associates, 1971.

Davis, Gordon B. Auditing & EDP. New York: American Institute of Certified Public Accountants, Inc., 1968.

Davis, Gordon B. Computer Data Processing. New York: McGraw-Hill Book Company, 1969.

Dearden, John; McFarlan, F. Warren; and Sani, William M. Managing Computer Based Information Systems. Homewood: Richard D. Irwin, Inc., 1971. 209-229.

Elliott, C. Orvelle and Wasley, Robert S. Business Information Processing Systems. Homewood: Richard D. Irwin, Inc., 1968.

Fletcher, Allan, ed. Computer Science for Management. New York: Brandon/Systems Press, 1967. 242-255.

Miller, Arthur R. The Assault on Privacy. Ann-Arbor: The University of Michigan Press, 1971.

O'Brien, James J. Management with Computers. New York: Van Nostrand Reinhold Company, 1972.

Sanders, Donald H. Computers in Business. New York: McGraw-Hill Book Company, 1968. 335-350.

Schlosser, Robert E., and Bruegman, Donald C. Accounting & The Computer. New York: American Institute of Certified Public Accountants, Inc., 1966. 145-182.

JOURNALS

American Institute of Certified Public Accountants, "Subtle Problems-Human Error Accidents, Responsive Controls--May be the Most Critical for EDP Installation Says Diebold Executive." Management Advisor. (September-October 1972).

JOURNALS

Brown, Harry L. "Current Problems of Real-Time Auditing." Management Accounting. (1969).

Brown, H. L. "Auditing Computer Systems." Management Accounting. (September 1972).

Carroll, John P. and Land, James F. "How a Bank's Internal Auditors Can Evaluate Purchased Software." Management Controls. (January 1973).

Eastin, Carol P. "Systems and Software Controls for On-Line Systems." Management Controls. (June 1972): 141-145.

Folsom, D. J. "A Control Guide for Computer Systems." Management Accounting. (August 1973): 49-55.

Grinaker, Robert L. "EDP and Internal Control." The Oklahoma CPA. (July 1965).

Harlan, Stephen D. "Providing for Effective Controls in Systems Design." Management Controls. (February 1973): 33-37.

Howes, Paul R. "EDP Security: Is Your Guard Up?" The Price Waterhouse Review. (Spring 1971): 47-53.

Louderback, Peter D. "Automating Internal Audits--for Banks." Management Controls. (April 1972): 69-72.

McReavie, Kenneth S. "A Conceptual Approach to Computer Controls." Management Controls. (July 1972): 166-173.

Moloney, Robert F. "New Generation EDP Control Considerations." Management Services. (March-April 1968): 15-22.

Moore, Michael R. "EDP Audits: A Systems Approach." The Arthur Young Journal. (Winter 1968).

O'Donnell, John J. Jr. "EDP and Auditing in Perspective." Lybrand Journal. vol.49. no.31968.

Peat, Marwick & Mitchell Co., publ. "Identifying the Sick EDP System." Management Controls. (September 1971).

Peterson, Norman D. "Error Control in EDP Systems." Management Accounting. (November 1970): 34-36.

Reider, Harry R. "Safeguarding Computer Records." Management Controls. (October 1972): 245-248.

Schomo, R. G. "Testing Internal Control in An EDP System." Management Accounting. (April 1973).

MAGAZINES

Chu, Albert L. C. "The Corporate Achilles Heel." Business Automation. (February 1, 1971).

"Fire Protection--The Methods and Costs of Protecting Data Processing Centers." Info Systems. (September 1972).

Henderson, Robert P. "Controlling the Computer's Threat to Privacy." Michigan Business Review. (November 1971).

"Key Punch Crroks." Time. (December 25, 1972).

Romberg, Berhard w. "Eyeball your Computer Operations Today." Info Systems. (December 1972).

"The Computer Thieves." Newsweek. (June 18, 1973).

TAPE

Weiss, Harold. "Computer Security and the Auditor's Responsibility." CPAudio #50. (1973).