1967

Management controls in electronic data processing

Francis J. Thomason

Management Controls in Electronic Data Processing

by FRANCIS J. THOMASON
Manager, Management Advisory Services,
San Francisco Office

Adapted from a paper presented before a joint meeting of the San Francisco Area Chapter of The Institute of Internal Auditors and the Golden Gate Chapter of The National Association of Bank Auditors and Controllers—October 1967

THE SUBJECT of discussion contains two elements—Management and EDP. Both have had a wide range of meaning applied to them. Since each reader would likely apply a different interpretation to these terms, the prudent course is to state the framework within which such remarks should be considered.

As to the term "management": Who is management and what levels of the organization structure should be concerned with EDP control? There are three general strata of the management structure who should be concerned with control of EDP. The first level in management structure to be concerned with control of EDP is the first-line supervisor—the person charged with day-to-day operation. The next is the first-line supervisor's superior, and the next is top company management. This last-mentioned group may occupy two or three levels in the organization. Subsequent comments will be directed primarily toward those controls that should be exercised by the first-line supervisor in either EDP operations or EDP systems design. They are of interest to the internal auditor because he is the representative of top management who must look at controls in an over-all perspective; and they are of interest to the controller because in many organizations the EDP function is located in his area of responsibility.

For the purpose of discussion, the term "EDP" must be circumscribed. In the term, we will include all types of installations concerned with processing information with mechanized or electronic equipment. The functions to be included are systems planning, systems development, programming, operations, scheduling, and so-called clerical control groups. The term "EDP," therefore, should be considered in a broad functional context.

Why should internal auditors and controllers as a group be interested in how management controls EDP? Some may even ask whether it is a proper concern of the auditor to question or observe the degree of

management control over the EDP function. The key reasons why you must become involved are three.

First, if your company utilizes data processing equipment in processing any financial or accounting data, the reliability of the accounting and reporting system is dependent upon certain controls. Outside sources rely heavily upon the internal audit function to assure themselves that all is well in the financial-data-collection, data-manipulation, and data-summarization processes. Investors, usually unknowingly, rely on you to provide certain safeguards; outside agencies, such as regulatory agencies, depend upon the internal audit function to perform certain basic tests of processing reliability; and the company's external auditors may rely heavily upon the work performed by the internal audit group.

Second, the internal auditor must become involved because the resources of the company become increasingly committed. With concentration of a company's data processing, strong controls are a necessity. Exposure to mishandling of data, whether the mishandling is intentional or not, is many times greater with EDP installations than in a manual or semi-mechanized processing system. All a computer can say is zero or one, but it can do it amazingly fast; and if it happens to be processing in an incorrect manner, it does that at fantastic speeds also. The consequences of incorrect handling therefore are too severe to tolerate; the processing controls must be such as to detect errors quickly.

The third reason the auditor must become involved is that EDP centers are becoming increasingly a vital part of most companies' operations. We cannot escape the consequences of the growth of information technology. This growth rate has been spectacular. It has developed from a small stream of unrelated jobs, such as billing or invoicing or payroll, to a virtual cascade of integrated jobs operating in real-time. We who have seen this fantastic growth over such a few years predict that we have only seen the bare beginnings of this burgeoning industry.

With the area of discussion defined and some reasons why you should be interested established, we may ask: What are some of the controls to be applied in managing the EDP function?

These controls can be grouped within categories that tend to describe their particular purpose:

General Management controls
Organization and Personnel controls
Documentation controls

Input-Output controls
Security controls
Programmed controls
Built-in controls

GENERAL MANAGEMENT CONTROLS

There are many actions that fall in the category of General Management controls, but essentially they condense to management involvement in the EDP function. There are over 20,000 computer systems in the U. S. today and, according to a recent survey, over half of them are not effective because of a lack of top management involvement. And, Mr. Auditor or Mr. Controller, this involvement must include you: *You* must know whether the EDP installation is operating satisfactorily; if you don't know, who is to interpret to your superiors? Some of the positive signs of management involvement are:

- Applications are planned, justified, and approved similarly to any other project in the company requiring commitment of capital or increased expenditures.
- Data processing techniques are applied to problems in different functional areas; i.e., marketing, accounting, engineering, customer records, etc.
- The EDP function is required to formulate general and specific plans showing where it is headed and what its plans are for the future.
- The EDP function is prepared to serve all functional areas effectively. By contrast, organizational placement sometimes tends to inhibit the EDP function to use by a single organizational group.
- The EDP function is staffed with competent personnel. Many EDP installations today are being supervised by competent technicians but inadequate managers. Who among you would buy a multimillion-dollar robot, turn it over to outstanding electronic technicians, and ask them to teach it to do many of your company's clerical processes, without regard for the selection or comprehensiveness of the processes concerned? And yet, this is precisely what is happening in many installations today. The EDP function must be managed—and that implies much more than the technical ability to make the machine run.

- Forecasts are required for equipment, personnel, space, and costs for periods beyond a year.
- Operating budgets are required for the current period.
- Management receives reports reflecting costs against budget; costs of specific programs are compiled; and costs are compared against some standard. As an example of comparison with some standard, one recent study indicated that successful EDP installations spend about ½% of their company's annual revenue on computer activities (equipment, systems staff, programming, and operating costs). That one measure, of course, cannot be the sole criterion of successful or unsuccessful operation, nor can that degree of expenditure necessarily assure success.
- Top management requires regular operational audits. It is here that most internal auditors and controllers would become directly involved.

ORGANIZATION AND PERSONNEL CONTROLS

The "organization and personnel" area of control now calls for attention. In the ideal situation, we would find a complete separation of the functions of systems development, programming, and operations. In very few instances, even in large data processing installations, is this practical. The reason is that to produce a sound EDP application, communication and co-ordination of effort is absolutely necessary between these groups. There are some procedures, though, that we should encourage; for example:

- Programmers should not be permitted to operate the computer during "live" processing. If they are familiar with a program, it is relatively easy to modify a processing step or alter data in a file and then correct the program or file to escape detection.
- Operators should not have a complete description of program steps available at the computer console.
- Operators should not be permitted to attempt program modifications to avoid an abort situation. Abort situations sometimes contain the exact clues to incorrect processing that should be called to a superior's attention.

In small companies, complete separation of duties is impossible, but this environment should make the auditor more alert to possible trouble situations.

One additional comment in the area of organization and personnel relates to training. A strong training program is extremely important, particularly in a small company. The vacuum created by the unexpected departure of a key operator, programmer, or analyst can border on disaster. The data processor is not immune to illness, family emergencies, the hazards of automobiles and trucks, or to the vibrant call of greener pastures.

DOCUMENTATION CONTROLS

The most widely abused, or ignored, area of control is in documentation. Documenting a procedure thoroughly is difficult work, but it is probably the most important area of control. Documentation is the road map of what the data processors claim is happening. It is a tool to be used for discussion with concerned parties; for providing a guide to the audit function; and for discovering where procedural weaknesses may exist. But most important, it should provide the point of reference for modifications in the system, whether by the original planners or by someone totally unfamiliar with the process.

Included in documentation are flow charts, block diagrams, procedure manuals, record layouts, form layouts, program listings, recovery procedures in case of equipment failure, a narrative of what is to occur in the processing, a listing of programmed machine halts, and computer log books or daily log sheets. Managers and auditors should insist on reasonable documentation. All the items just enumerated must be prepared at least in limited form before any process can be operative. Isn't it reasonable to require that it be done in a competent and professional manner? Without these basic tools there cannot be adequate communication, adequate management review, concise modifications, adequate operating personnel training, adequate procedural review, or adequate error analysis.

Despite these valid reasons, documentation, as aforesaid, continues to be the prime failing of most EDP installations. In the writer's opinion, this failing is also the prime reason for ineffective EDP departments —because they mire down immediately when trouble strikes.

Documentation standards should be developed within a company so that uniformity of expression will exist between analysts and developers; also, to aid in procedural review. The standards should be expressed in terms of instructions to analysts and programmers, and the standards

should be enforced through frequent review by the EDP manager and the audit department.

INPUT-OUTPUT CONTROLS

In reviewing an EDP operation, we anticipate finding a clerical group charged with preparing and/or reviewing input and output controls. These controls generally relate to assuring that all data are processed by the data processing department. This assurance is gained by comparing some total furnished by the customer department to a total generated in the processing cycle. These totals are ordinarily based on source documents and can be the total number of documents or a total of some data field from the source documents.

The control group also usually maintains some type of control data over master files, such as the number of records in the file and the year-to-date totals of specific data fields.

Also, the control group normally is charged with reviewing output reports for accuracy before their release. The basis for this checking can arise from several sources, but usually is a combination of file totals prior to processing, the input controls mentioned previously, and the file totals subsequent to processing.

If the input-output control group is not an integral part of the data processing operation, the auditor should pursue the matter and determine whether the control function is being performed by the customer departments.

Two incidents coming to attention recently illustrate that even simple protective methods are not always utilized in internal control. In one case, a very simple review would have shaken an auditor's confidence in the data being prepared and reported; in the other, an auditor would have been shaken because of the lack of protection against wrong doing by a computer operator.

In the first instance, the company had changed from posting customer ledger cards by posting machine to a data-processing-service-bureau operation. After about three months of operation, the chief bookkeeper reported to the auditor that the sum of the detail ledgers did not agree with the general ledger control account. The general ledger account had been posted with daily totals. Upon investigation it was determined that the totals of the daily posting to the detail accounts were not being compared to the amount being posted to the general ledger con-

trol account. Strangely enough, customers had been calling in and reporting discrepancies in their accounts and were being told that it was "probably due to the processing change and that it should come out all right in a month or two." A simple daily procedure would have saved many hours of labor in finding and correcting the errors and, what is more important, would have protected the company's public image. Elementary, perhaps, but the steps to assure correct processing were not taken.

In the second case, a small number of items clearing through this bank each night would fail to be processed by the EDP operation because the account number was illegible, because a check or document was mutilated, or for some other normal or plausible reason. These items were corrected and re-entered in the following day's business. In this situation, a control total was developed each day, with the unprocessed items being considered properly. The data processing operation was relatively small, and the same person normally operated the computer each day. The something lacking was that no one ever inspected the unprocessed items, and so the operator's personal draft could be concealed among the unprocessed items for days at a time. That operator had "control" of his processing operation!

SECURITY CONTROLS

In the province of security controls, it is necessary to distinguish between "physical" security, "data" security, and "operations" security. The main emphasis in the data-security category is on control over the data. In one experience, substantial rerun costs were incurred because of the destruction of a master file. In this case, the header label check, which gives the operator an indication of whether or not a tape reel may be written upon, was deliberately suppressed. The reason given was that the minute or two required to print the label check on the console was "costing money." This kind of "logic" resulted in a rerun cost that would pay for typing the header label check several thousand times.

The protection of disk files or packs has created a problem among users. One practical solution is the periodic writing of the disk file or pack onto a reel of tape. The material cost of the tape is negligible when compared with the nonproductive unload time. This nonproductive time is a factor that must be considered in determining the best method of safeguarding data.

In an operation where tape master files are utilized, the normal procedure is to retain outdated tapes for a period of time. This leads to the terms "son," "father," "grandfather" master file tapes.

More recent developments in data processing make it possible for a person many miles removed from the computer to make changes to files via remote terminal devices. This situation must be controlled through use of access or "right-to-look" coding, so that unauthorized persons cannot modify files or obtain data to which they are not entitled. The means of assuring control over this type of access will require thorough investigation by the auditor and positive tests of control processes.

In the category of physical security, the auditor should be alert to the protection afforded equipment and files, such as adequate fire protection, protection against intentional destruction of certain files, and the use of off-site storage of records or tapes, thus increasing the chances for recovery from catastrophe at the main site. Copies of program listings should not be overlooked when deciding upon items to be needed for emergency recovery.

When thinking about security controls, there are a number of items related to operations that should not be overlooked. For example, the console output log should be inspected by the operations supervisor to find indications of problems. The auditor should also occasionally check these logs; the presumption is, of course, that the logs will have been printed with meaningful terms and not as a jumble of unmeaningful characters.

The operating personnel should also be rotated from job to job to minimize any risk arising from an operator's becoming too familiar with a particular application and its associated routines.

Machine utilization statistics should be collected periodically to obtain performance statistics, to control unproductive time, and to assist in scheduling operations. Operations personnel may object to such collection of data, but this information can be extremely informative and useful in managerial control of equipment operations.

So much for security controls—physical security, data security, and operations security.

PROGRAMMED CONTROLS

Programmed controls are also known as processing controls or programmed checks and are a part of the internally stored instructions

directing a computer's operations. Thus it is possible to make the computer self-regulating and thereby eliminate the need for extensive clerical monitoring. The extent to which programmed controls are used is primarily a matter of weighing the costs of developing the programs against the costs and results of not utilizing this technique. Some costs and effects of not using programmed controls are difficult, if not impossible, to measure; and therefore the degree to which they are to be used becomes a matter of judgment. Sometimes, because of the additional programming time required or the expansion of a program beyond memory capacity, the decision is to ignore or minimize this strong control technique. Whether or not this decision is one of simple expediency should be determined.

Some programmed controls relate to subject matter discussed previously, such as the establishment of preprocessing batch control totals. These methods can be utilized under program control with the computer doing what would otherwise be a clerical operation. Record counts are used extensively in programmed controls and can apply either to detail records being processed or to master files. Record counts are easy to program, require a minimum of additional storage space, and add practically nothing to processing time. Record counts, however, do not control the correctness of records nor do they isolate records that may be incorrect; other techniques must be used to supplement the record-count technique.

Control totals of groups of records is another widely used programmed control, especially if a balance-forward operation is concerned. A favorite method used to establish the control amount of detail transactions is to program the initial or edit-run of transactions to accumulate this total and then carry it forward into the updating run.

Under computer programming many other quantitative control techniques are possible. The point is that the computer can be used to perform work of a quantitative nature to assist in controlling the data processing operation.

Besides quantitative controls the computer can be programmed to develop qualitative controls. These qualitative controls relate to the data content of records. They test the consistency of record arrangement, the presence or absence of specified items of data, and the reasonableness of certain kinds of data. A simple example of qualitative control may be helpful. The computer can be programmed to check data input

combinations and to indicate a discrepancy if the incorrect combinations appear in data to be processed. Assume that there are a number of salesmen, each assigned to a separate sales territory. Thus if sales record input data indicated that salesman A had made a sale to a customer located in salesman B's territory, the input data could be selected for inspection and correction if necessary. For this purpose many companies carry the salesman and territory numbers as a part of a customer's master record.

Another type of programmed control is used exclusively to control operator functions. The machine operations are generally conceded to be highly dependable, but this is not conceded with the operator's actions—so one method is to program the machine to check his actions. For example, important records may be destroyed unintentionally by placing the wrong reel of magnetic tape on an output drive. It is also possible to process a transaction tape, mistakenly, more than once, to update a superseded master file tape, or to fail to process one or more reels of a series of transaction tapes. These are serious errors because they create operating delays and can create inaccuracies in the records that are difficult to detect and correct. Work rules and tape-handling instructions do not always prevent these errors, and an internally programmed check is therefore needed to detect an error in mounting tape reels. This is done by recording a magnetic label at the beginning of each tape reel and then comparing this label with an identifier previously loaded into the computer or with an identifier resulting from the last processing. If the labels do not agree, the machine can be programmed to halt and discontinue processing or to print a message to the operator. Sometimes the label numbers are printed, even if they are correct, as evidence that the comparison was actually performed. Another programmed control is printing of messages and programming check points into the processing program. In these instances, all machine halts or error messages should be indicated on the console printer and a copy sent to the audit department. In many situations this copy would provide only a psychological control, but it would provide a trail and give assurance that the procedure was being followed.

So much for programmed controls. But remember this technique and its availability for utilizing the computer to assist in controlling its own operation, and take advantage of its capability to do so.

BUILT-IN CONTROLS

Computer manufacturers, recognizing that malfunctioning may occur occasionally in a computer system composed of many parts, have provided built-in controls enabling the machines to detect automatically the more common types of errors. Normally, these controls are always operative and are not subject to program or operator interference with their performance.

As an initial example of built-in controls, magnetic tape units utilize a technique called parity checking, in which the computer counts the number of magnetic bits, or spots, on the tape and can tell by certain combinations when a bit is missing or has been added.

Another built-in control is the technique of reading a record after it is written on magnetic tape and of comparing this reading with what was intended to be written. This is called the "read after writing" feature.

There are many of these built-in controls, such as "echo readings," "interlock circuits," "duplicate circuitry"; but they are of interest to internal auditors and controllers only to the extent of recognizing that they exist.

FUTURE

This discussion would be incomplete without looking briefly at what the near future will require from management and from the auditor. Three recent significant technological advances will have a tremendous impact upon the EDP function:

- The ability to store huge amounts of data economically and retrieve the data quickly, giving rise to the term "corporate data bank"
- The ability to process vast quantities of data at fantastic speed so that the computing cost per unit of data processed is coming within the economic reach of even the smallest company
- The ability to put factors into data banks or retrieve factors from data banks from remotely located terminal devices

These abilities are NOT for 1985; they are possible NOW; the concepts have been reduced to operational capability NOW.

As a consequence of these advances the internal auditor may soon be forced to cope with such things as the absence of source documents;

data being processed in real-time (that is, without time lag for reviewing results before proceeding); and a less visible audit trail than today.

SUMMARY

In summary, a company's management has a grave responsibility to understand what is happening in the EDP function. And the company's management will expect that the internal audit function assist them even more than ever before in assuring that the data processing function is being conducted in an efficient, correct, and dependable manner.

The company's management, including the internal auditor, must prepare itself to understand what is happening; if they do not, they will abdicate their responsibilities. The auditor will be forced to be more visionary, imaginative, and knowledgeable if he is to cope with this new way of life.

There is no reason why management cannot continue to maintain strict control over the EDP function. Hopefully, at least one new idea to achieve this control has been suggested. We cannot stop, nor should we attempt to stop, this technology that gives us the ability to multiply the power of man's mind. As auditors and controllers we must be prepared to utilize this technology properly, take advantage of the opportunity it offers, and advance contemporaneously with it. The future holds great challenge and excitement for all who are not dismayed by the prospect, but, instead, launch into it with eagerness and the thrill of exploration.