Auditing magnetic-tape systems

By John V. Goodman*

This paper is based on a talk given to the Birmingham branch of the British Computer Society on 11 December 1963. It reviews the changes in approach to auditing large volumes of data processing work, and tends to the view that the work will ultimately be more easily controlled with systematic magnetic-tape systems, than with large updated random-access systems.

Background

I think it would be fair to say that the approach of the auditor to his work has changed over the years with the development of large commercial enterprises and involved systems to cope with their clerical work. In the early days, after a somewhat rudimentary look at the system of internal control, the auditors would proceed to very extensive detailed checking—in some cases to every transaction in the books. Over the years, auditors have tended to pay far more attention to internal control, and the weaknesses, or lack of them, in any system have formed the basis of their tests. With each new development, either of systems or accounting machines (and these developments have nearly always tended to reduce the accessibility of the "audit trail"), the auditors have had to sit down and take a global view of precisely what it was they were trying to accomplish.

At the risk of stating the obvious, I would suggest that auditors are in fact aiming to be able to state once a year that the financial accounts presented to the shareholders—their responsibility lies with the shareholders not the directors—present a true and fair picture of the state of the company and the profit or loss it has made. Coupled with this is the fact that the accounts should be prepared on a basis consistent with previous years, unless otherwise stated. From this, it is obvious that the auditor must be satisfied about the accuracy of the accounts and the absence of fraud, before he can give his certificate.

Viewed in the light of these developments, the advent of E.D.P. is only another step in a very long trend. The only new problem is that it brings in a new technology, which the auditor cannot pick up without specialized training and probably is most reluctant to have to acquire. The trend towards much smaller computers, for medium-sized companies (as opposed to industrial giants), means that the problem of auditing E.D.P. systems will not be, and is not, confined to the very large firms of accountants. These latter firms normally deploy a large staff on their bigger audits and thus have less of a problem in finding specialist staff to deal with E.D.P.

Trend

There were many misconceptions during the "magic brain" era by auditors who thought that there would be nothing left to audit! In practice the needs of management for control, and the need for a step-by-step approach to E.D.P., has enabled auditors to prepare themselves. This certainly has been the case in the U.S.A. I, personally, do not know of any case where a company has jumped from a fully-documented system to a completely integrated system having no visible source documents. The trend is obviously to reduce source documents, but we can hope that the auditor will have been prepared for this by a year or two of an "application by application" approach.

Internal control

I have mentioned the trend towards greater attention to internal control by the auditor in recent years. This is usually accomplished by a questionnaire technique, coupled with tests, to prove the accuracy of the answers the auditor receives. What is internal control?—I feel I must quote the following, at the risk of boring the reader:

> "A division of duties among the employees of an enterprise in such a manner that no one person has complete control of any important business transaction and that the work of each employee is checked by another employee carrying out a successive step in the same or related transaction, to the end that the company's assets may be protected against misuse and fraud, and reasonable accuracy of the recorded transactions and of the reports thereon be assured."
>
> Essentially—segregation of responsibility.

This definition, when applied to an E.D.P. system, suggests that the machine operator is the weak link in the set-up. He or she is responsible for a vast amount of work, and by means of the console, specially-introduced punched cards, tapes, etc., could conceivably carry off a major fraud. This is particularly so if the operator is also a programmer. Some people scoff at this idea, as computer personnel do not normally associate with accounts staff, or have access to accounts records. A programmer or operator could, however, be unwittingly used as a tool of a manager, who might try to pull the wool over the eyes of the auditors. An example of this might be a program designed to print out for the auditors a list of items from a master stock file held on magnetic tape, which were two years old. The program could easily be altered to show only twenty-year-old items, and the auditor would have no Kardex to

* *Honeywell Controls Ltd., Moor House, London Wall, London E.C.2*

refer to! This sort of fraud is rare in Britain, but only recently in the U.S.A. a vice-president of a brokerage house was found to have punched up cards, after hours, and left them to be credited (in a punched-card installation) to various accounts in which he was interested, the following morning. I mention these cases to point out that the auditor must not rely on the superb accuracy of computers, and the air of "separateness" to be found in most machine rooms!

Good internal control should probably involve all or some of the following:

1. *An independent controls department*

This department is most important and would prepare pre-lists of input documents including "hash" totals of descriptive information and record counts. It would be responsible for receiving control totals prepared by the computer, and checking the reconciliations (which should be made a part of every updating run) to prove the accuracy of balances carried forward. A careful balance has to be struck here, as elsewhere, between the cost of control and the associated risks of dispensing with it.

2. *Machine room control*

Included under this heading would be control on operating time and personnel time; more than one operator if possible; rotation of operators, so that one program is not always handled by the same person, and separation of programmers and machine operators.

3. *Strict control on the program library*

4. *Physical control of magnetic-tape files*

This would include proper labelling and indexing, records of usage and use of the "grandfather, father, son" technique to be mentioned later. The write-inhibit ring protection feature, which prevents inadvertent erasure of data on magnetic tape is important.

5. *Programmed controls*

I will deal with these at length. This type of control is built into the computer program by the systems man, and is performed by the computer itself. Because of the high reliability of modern solid-state computers, and the consistent manner in which the computer treats data, the programming logic and check-out techniques of the system are the significant factors, once input accuracy is assured. It seems unnecessary to perform double arithmetic internally, or to compare the number of items entering the system with the number leaving the system (as in sorting or in a file-updating situation). If the program logic is sound, and the program is thoroughly checked out with live as well as test data, and if an adequate parallel operation (running both the new and old systems and comparing the results) is performed, this type of internal checking is superfluous. It is true that an unusual combination of conditions can occur which could cause an operating program to go awry, but this is rare and the condition will most probably cause the program to "hang" and thus signal the error. Emphasis should be placed on assuring the logic and consistency of the program, rather than controls to check internal computer operations.

Within this context, however, the control of input is very important. The saying that a system is only as reliable as the accuracy of the input is certainly valid. The converse theory of *Gigo* (garbage-in, garbage-out) is equally valid! It is in this area that a computer can make a very significant contribution, and can ensure a degree of input accuracy hitherto impossible.

Batch totals

One of the most common control checks is that of batch controls, whereby an independently-produced batched input total is compared with the total of the same batch produced at some later point in the processing. Batch totals are primarily used where data physically move from one point to another in the processing, e.g. data on punched cards. Computer operation, with the ability to integrate systems and processing, greatly reduces the need for the batch total type of checking.

Label checking on input files

In addition to the visual gummed label placed on a magnetic-tape reel, there is another programmed label check that can be performed. A label record is written by the computer on the recording surface of the tape. A programmed control can then check this label, to determine if the proper tape is mounted for subsequent processing. Thus the programmed control can check the physical operating control.

Limit checks

A limit check on input can be incorporated to ensure that only valid codes or transaction types are permitted. For example, if there are only five transaction types, a limit check will indicate if a transaction other than one of the five is encountered (an error situation). Transpositions can be detected if one figure is not valid. After programmed controls, I would add two more features of internal control:

6. *Proper security features in the hardware*

I will mention these briefly later; and

7. *Control on console type-out*

The typewriter record of the console Flexowriter or electric typewriter (if included in the system), can be a most significant control if properly handled. The console typewriter records all instructions and data manually entered into the computer. It therefore can be used to trace any action of the operator which might affect an operating program. The console can also be

used by the programmer to type out messages for logging and monitoring purposes. For example, a standard procedure for an installation might be to type out the name of the program being performed, the date, the tapes being used, messages noting any error or special situation and the successful conclusion of the program. The console type-out can then be saved and used as a log and control for the operation. Several procedures must be followed if the console type-out is to be an effective control. First, two-part paper with sequence number control should be used. Another alternative, although a more expensive one, is a locked slave console which operates in parallel with the main console, but whose print-out would be under lock and key. Secondly, a distinction between production running and program checkout should be made. During checkout, there are frequent console type-ins and type-outs, which are only intelligible to the programmer, and would be too lengthy and confusing if kept as part of the log.

The auditor will investigate the system of internal control in use, and having done so will decide the scope of his examination. He will have to take into account the availability of an audit trail, source documents and printed output. He can then decide to what extent he will test the running of the system (a systems or procedural audit), or will examine specific transactions on their path through the system in the conventional manner (via the audit trail).

It is obvious from the above that the auditor must be involved in the E.D.P. system from its inception, and, more important, should be in a position to discuss his needs before the order is placed.

Magnetic tape

I think the last point can logically take us on to consideration of magnetic-tape systems.

I hope to be able to confine myself to the advantages of magnetic-tape systems as they affect auditors, and I do not think it is within the scope of this paper to discuss the ever-present problem of serial processing versus random-access argument.

Costs, reliability and speed

The auditor will be affected by costs of magnetic-tape systems, to the extent that any additional information required by him either temporarily or permanently will cost money. Leaving aside considerations of storage space, you may not realize that compared with magnetic tape, the cost of storing an equivalent amount of data is six times greater on punched cards, from 20 to 60 times greater on random-access devices of the disc type, about 30,000 times greater on magnetic drums, and from 150,000 to 600,000 times greater on magnetic-core storage.

The very high reliability of certain magnetic-tape systems will be a surprise to auditors used to punched-card systems. This is of very real concern, if they are to base their audit on limited tests of the system.

The speed of magnetic-tape systems (for example, the equivalent of 96,000 decimal digits can be read or written per second on a *standard* Honeywell system) will affect the auditor, to the extent to which he will want duplicate tapes or audit programs written and processed.

Error checking techniques

The auditors will want to know what error-checking techniques are available as part of the hardware of the system. These include:

1. Memory (store) parity checks.
2. Internal logic checks.
3. Card read or punch checks.
4. Validity check on cards read.
5. Printer echo-check.

These will of course apply to all E.D.P. systems. I do not think the auditor can hope to judge the efficiency of these.

Tape systems have various forms of error-detection techniques based on lateral and longitudinal checks. This is because even in the best controlled and air-conditioned system it is possible to get dust on tapes. (For example, the Honeywell *orthotronic* control system not only detects these errors, but corrects them without manual intervention or lost computer time.) The regeneration procedure, or ability to recover data from faulty tapes, is a very important feature, from the security aspect.

Strengthening internal control

A magnetic-tape system may, in fact, be capable of strengthening internal control by recording and retaining (at low cost) information previously found uneconomical to compile or store by other means. Such data can be used to show up unusual situations on an exception basis.

In addition, it is completely feasible on magnetic tape to retain the history of all transactions at low cost, for as long as storage space can be provided. This operates both to the advantage of management and the auditors.

Magnetic-tape systems imply serial processing of data. Under this technique all the items in a master file are normally examined and updated each day (or week). This cuts down the possibility of delays in recording information, and speeds up exception reporting on critical items, which may not have been affected by input data, i.e. all items can be scrutinized daily, not just the items which have moved.

Also implied by a tape system, is breaking down the work into simple program segments at each of which control totals can easily be produced, if control is improved thereby. The entire batch of these segments is treated as one unit. The transition from program to program is virtually automatic, thus cutting down on the possibility of errors.

The "grandfather," "father," and "son" technique for retention of magnetic tapes effectively guards against malfunctions of equipment. The input tape is of course not overwritten during a run, and strict controls can

be instituted to prevent its re-use until the proper time. Thus, it should always be possible to regenerate information, without undue difficulty, should this be necessary.

Master files can be reproduced for the auditor easily and quickly, and can be produced during the operation run if a spare tape deck is available.

The label record written on to the beginning of the magnetic tape by program acts as a double check that the correct tape is being read. This label can contain descriptive information and void-date designation, which will prevent it being used before some specified date or other criteria.

The audit program(me)*

Having completed his review of internal control, and investigated the magnetic-tape system in use, the auditor has various approaches to his programme of work:

1. Test the E.D.P. system with his own computer program. On a surprise basis, he would attend during the running of a program and on completion would re-run the same program with test data which would provide known results. The test data produced during the debugging stage would be used, if it can be salvaged. The restart feature, if satisfactorily provided by the system, is useful here, as the auditor does not need to worry about derailing the program. He may introduce arbitrary data, which should fail some existing limit on the program, in order to test its continuing validity.

2. Provide for features to be written into the operational program for audit purposes only.

These sections of program would be called in at the option of the auditor on demand, and could produce print-outs of series of items in which he is interested. There is an obvious lack of secrecy here, however.

3. Trace routines can be used to follow the path of a particular type of item, and print out each change of sequence.

4. The ultimate goal—*an E.D.P. audit program.*

The advantage of this step is that the auditor's program can be secret as are (or should be) his more conventional programmes.

* It is a convention of this *Journal* that "program" means a series of computer operations, covering a procedure, whereas "programme" means any schedule.

No one will underestimate the cost of preparing such a program. To illustrate what such a program would do, however, I will mention work done in the U.S.A. by a large firm of accountants. The application was a large payroll. They attended one month, and in their presence a duplicate of the master file was made on magnetic tape, of which they took possession. One month later the same procedure was adopted. Their program was then run to extract from these two files details of new employees, terminations and rate changes. Tests were carried out checking rate paid against rate code, etc., and exceptions printed out. Conventional audit checks could then be carried out on the printed data.

Conclusion

In summarizing the wide field I have attempted to cover, I think it is obvious that auditors or specialists in their firms must begin to know a good deal about computers. I doubt whether they need to be programmers, and some may even disagree with me that they must have staff competent to frame an internal control questionnaire, investigate and audit a system. The advantage that auditors have now is that they should have surmounted their problems with the more routine applications, before the next more integrated phase of E.D.P. evolution is reached. When we reach the stage that visible source data is reduced to a minimum, coupled with fully integrated systems, it seems that auditors must then have their own E.D.P. programs, since previous methods will not be available or suitable. The ease of handling such programs on magnetic tape, and the economy aspect, lends weight to the other features of tape systems which should appeal to auditors. As mentioned previously, auditors must obviously take some part in their clients' E.D.P. deliberations, at an early stage, and at the latest stress their requirements before programs are debugged.

Auditors obviously need to be more readily available during the course of a year and their work will in many cases have to be done at the same time as or shortly after production runs.

The result of this closer contact must surely result in a better service to his client who will gain considerably from the knowledge the auditor has of the problems of his business.