

Audit test packs and computer audit programs

A. D. Chambers

Graduate Business Centre, The City University, Gresham College, Basinghall Street, London EC2V 5AH

The different roles of the internal and external auditor are examined, together with the principal methods of sophisticated computer auditing. Test packs and audit programs are discussed and problems posed by auditing on-line and real time systems.

(Received September 1974)

The law requires the external auditor to satisfy himself that the year-end results to be published show a true and fair view of the state of affairs at the end of the year and of the profit and loss for the year, and that these results are in agreement with the books of account which have been properly kept.* The work he does to be in a position to make this report to the shareholders, largely boils down to *procedural tests* and *verification work*. In his work on the procedures of the company he is of course only concerned with those procedures which influence the financial results of the company: he must first ascertain what the company's procedures are *alleged to be*, then test whether they are *operating satisfactorily* and finally conclude whether they are *adequate* to ensure a true and fair view. Since he has the shareholders' interests at heart it is theoretically possible, though unlikely, that the external auditor could make demands for modifications to procedures (e.g. provision of additional audit trail) which would not be strictly necessary for day to day management purposes. This would never be the case with the *internal* auditor who offers management an independent appraisal of the effectiveness of internal control: if the internal auditor concludes that modifications to procedures are required he does so because in his view the modifications to procedures are required so that management is placed in a better position to manage effectively. With respect to their procedural work the activities of the internal and external auditor are therefore broadly similar except that (a) the external auditor may make 'demands' which are not strictly essential for the management of the organisation, and (b) the internal auditor is concerned with all operations of the organisation, not just the financial operations.

Audit trail

It is a false argument to suggest that the procedures of a computerised company are contained in the computer program listings of the company and that therefore the auditor must be competent to read computer documentation. The actual procedures of a company are 'what the company does'. The auditor has always been obliged to commence by ascertaining what the company's procedures are *alleged to be* and his approach (whether with manual or computerised systems) will be to talk to staff, read clerical procedures manuals, and so on. He should have no need to examine computer program listings to determine what the company's procedures are meant to be. The program listing is not in any case what the computer actually does: this is determined by the logic held on magnetic store which is quite unreadable by anyone. The only way an auditor can satisfy himself that the organisation's official procedures are in fact carried out (whether by a manual or a computer system) is to design and conduct tests, and the most satisfactory way is to test sample transactions by reference to the audit trail left behind when these transactions were processed.

*The Companies Act, 1967, Section 14

Audit trail is the preparation and retention within an organisation (a) for an adequate period (b) in a reasonably accessible form and (c) in enough detail to satisfy the auditor, of records which allow each detailed element of any transaction to be tracked from its source through each intermediate stage to its final disposition(s) whether in detailed or summary form or both; and vice versa (i.e. the facility to use records to trace back in detail from the final outcome(s) through the intermediate stages back to the initial source(s) of transactions).

If the audit trail is adequate the auditor can usually get away with a 'black box' approach to a computer audit; that is, he can audit round the computer and not get involved with what actually happens in the computer room beyond satisfying himself about the standard and security of operations, the segregation of duties and such like. If the audit trail is not adequate for the internal auditor this means that the records of the organisation are inadequate for management to manage effectively for, as has been said, the interests of management and the internal auditor are the same. While on 'first time through work' the internal auditor may have to resort to alternative and relatively sophisticated computer auditing methods (discussed below) in order to make up for a deficiency of records, he should not have to do so on subsequent audits of the same system. By the time these later audits occur management should have remedied the deficiency in the interest of better management.

If the internal auditor may therefore occasionally have to resort to special computer auditing techniques then the external auditor can expect to have to do so more frequently. The external auditor may not always be able to persuade management to increase the amount of audit trail: this is likely to be the case where the records are requested purely for statutory audit purposes and are of no advantage to management for management purposes. It can be argued that management should not adopt this attitude as management is in a fiduciary relationship to its shareholders as well as being legally obliged to assist the statutory auditor, and it is as much management's responsibility to fulfil its obligations in this direction as it is to manage efficiently. External auditors should certainly argue in this way but in practice they may expect to be posed more inadequate audit trail problems than may the internal auditor.

Verification work

If procedural tests require sophisticated computer audit techniques, then verification work certainly does. However good the audit trail there may be no satisfactory alternative on to employing special advanced computer audit techniques on verification work. Although it is true that the *internal* auditor is not employed to report on the published results of the organisation as is the statutory or external auditor, he may however to a lesser extent get involved in some verification work. To that extent he must be a master of the appropriate advanced computer auditing techniques. A satisfactory audit

of the procedures of the organisation will enable the external auditor to conclude on the amount of confidence he has that the year-end figures have been built up correctly during the course of the year. He must however test selected year-end figures directly, and this is called verification work. He may need to extract a quota or random sample of debtors' balances to do additional work on the sample balances so as to prove them. He may need to explore relationships between data held on different computer files to check whether they are compatible or reconcilable. He may be interested to classify ledger balances by size or degree of activity. The internal auditor may need to do similar work although his work will not necessarily be geared to the year-end results. None of these special verification tasks may be pursuits which management themselves might want to undertake from time to time: in view of this management cannot normally be expected to provide the computer system features which would facilitate this work. So the auditor must provide them himself and in fact the external auditor would generally wish to do so to maintain a degree of independence and confidentiality in his work.

Test packs

There are two principal sophisticated computer auditing techniques: *test packs* and *computer audit programs*. Test packs are test data prepared by the auditor and processed by the operational computer programs of the system being audited so that the results so produced by the computer may be compared with manually predetermined results and discrepancies explained. Despite the effort involved it is a mistake to dispense with working out manually what the results are expected to be: it is surprising how many invalid results may be overlooked when the scrutiny of the test pack results is not by means of a comparison with what has been manually assessed as being expected. The term 'pack' refers to the deck of cards conventionally used to input the test into the computer system. In reality the test will often commence with the source documents from which the cards are subsequently punched as this extends the audit test to cover the standard of key-punching. However it is more important to define precisely the objective of the test and resist the temptation to embellish the test with a series of subsidiary inessential tests. Today punched cards are being replaced by key-to-tape, key-to-disc and computer controlled data preparation not to mention the devices which read marks or characters, whether optically or magnetically, direct from appropriate source documents: in these circumstances there is no alternative to holding the test pack as a pack of documents rather than a pack of cards. The special considerations which apply to the audit of *on-line systems* (which may or may not be *real-time systems*) are discussed later.

Test packs confirm whether the computer programs process the submitted data correctly. The opportunity exists to submit invalid as well as normal data to test error and exception routines. With regard to correctness it may be as important to test for *completeness* (is all data processed?) and *duplication* (is any data processed more than once?) as it is to test for *accuracy*.

Test packs would be used when conventional tests were inadequate due to, for instance, loss of audit trail. The trouble they invariably cause the computer and computer user departments should be enough to deter auditors from indiscriminate use. The pack should be submitted as part of the standard live data stream whenever possible: if this is not done the auditor will have less confidence in the results; if it is done the inconvenience to the client is likely to be greater. Certainly the client must be involved even though this reduces the element of confidentiality inherent in the test; but it does avoid many of the risks associated with the auditor using the live system.

There is no need for the client to be appraised of the finer details of the test. The sequence of steps the auditor should follow when he uses a test pack is:

1. Define the problem
2. Involve the client
3. Obtain computer documentation
4. Open audit working papers
5. Construct test data
6. Predetermine results
7. Attend the computer run
8. Check and summarise results.

Test packs have many advantages. Usually the audit test so performed is a good, thorough test. The pack is quite cheap to set up and once set up may be virtually permanent requiring only detailed modification for use on subsequent audits. It is certainly cheaper to run in terms of computer time than is a computer audit program: this is due to the test pack usually being slotted into the live job stream thereby avoiding the 'set-up' time which would be associated with a special computer run. The element of risk to the client's system is real but not so great as the risk borne by the use of computer audit programs. A program is more likely to cause great damage (e.g. by overwriting client master files or running riot through the disc-based program libraries, etc.) than a pack of data. Finally a test pack has the advantage that it is portable and may be taken away by the auditors at the conclusion of their audit so that physical security is assured.

Test packs do however require quite a detailed grasp of the computer system. It is difficult for laymen to understand computers and undoubtedly this bars many auditors from availing themselves of this auditing technique. A further drawback is that test pack data may have to be prepared and processed through parts of the system that do not warrant testing in this way. For instance it may be necessary to set up some dummy customer master file records so as to be able to use a test pack of dummy incoming orders. So long as the pack is part of the live job stream one can generally ignore the computer time it takes. However sometimes the client will be involved in programming time with its associated computer time. This may be essential if it is decided to use the live job stream but nevertheless it is essential to suppress certain processing steps which the test pack would otherwise cause. For instance it will frequently be necessary to ensure that a stock file balance is not adjusted to reflect customer demand as contained in a test pack of dummy orders: if this balance were adjusted this might result in bona fide customer orders being rejected due to incorrect out-of-stock information being held on the computer—and the test pack would be to blame. Similarly control totals and ledger posting totals may be distorted by audit test pack data. Sales or other analyses may also be thrown out of true. Occasionally, unless program amendments are made to suppress unwanted side effects of audit test packs, physical consequences may occur of an unexpected nature—as when an audit partner (whose name and address had been used in a test pack to create a dummy customer account) had several van loads of furniture delivered to his flat. The alternative to programmed amendments designed to detect audit test data and avoid untoward consequences is to notify line management in all areas of the company affected so that manual adjustments can be made to computer output. However this will not be practical in most instances when the computer's automatic responses have been modified by the audit test data—as in the example of out-of-stock situations occurring after an audit test pack of dummy orders had been processed. It is worth remembering that one test the auditor may frequently wish to make will be a volume test designed to ensure that the computer can correctly handle exceptionally large quantitative or monetary amounts: the

impact of such tests will of course be proportionately disastrous unless anticipated and dealt with.

One way to avoid most of these consequences is to process the audit test pack against a copied version of the computer files. If this is done care must be taken to ensure that earlier generations of the files are not used if these are still needed for back-up purposes on the 'grandfather-father-son' principle. Additionally, care must be taken to ensure that *all* the files which are mounted to process the test data are copy files: it is easy to overlook a file or two and thus corrupt the live data held on them. It may be, for instance, that a sales analysis tape has been added as a refinement to a program but this has not been documented in the system documentation which the auditor is using and is therefore unknown to the auditor. An advantage of using copies of files for the audit test is that physical control of these files can be maintained for as long as is needed by the auditor so that any matters arising can be checked out thoroughly if necessary by rerunning the test pack against the same files at a later date. This is more practical with tape files than with disc files as in the latter case several logical files may be held on one physical disc pack and it is in any case rather impractical for the auditor to take physical control of a disc pack costing often over £200 as against £10 for a magnetic tape.

The main disadvantage of using copies of files is that the test pack is no longer part of the live job stream and it is consequently a weaker test as the auditor cannot have so much confidence that the day to day live data would be processed in the same way. It has been known for a company to retain an old version of an important program especially for the external auditor. The client remembered the nail-biting experience of the auditor in designing his test pack in the first place, and innocently considered he was rendering the auditor a service in allowing him to run his test pack in subsequent years against a superseded version of the program which bore increasingly less resemblance to the current version. It took several years before the auditor by chance discovered what was happening.

The above example illustrates that there may be no proof that the current, operational program has been tested. Similarly there is never absolute proof that live data would react in the same way. Fatuous though it may seem it is possible that the operational program could detect the transactions which were the auditor's test data and process these dummy transactions in the correct way while conducting some jiggery-pockery on the genuine, live data. The auditor would rightly counter by pointing out that such a practice would suggest fraud, and, in the classic words of Lord Justice Lopes (*In re The Kingston Cotton Mill Co., Limited, 1896*): 'an auditor is not . . . a detective. . . He is a watch dog, but not a blood-hound. . . If there is anything calculated to excite suspicion he should probe it to the bottom, but in the absence of anything of that kind, he is only bound to be reasonably cautious and careful. . . The duties of auditors must not be rendered too onerous.' However, without any suggestion of fraud, it may well be the case that the test pack is an inadequate test of the system as facilities may exist within the programs which are unknown to the auditor and may therefore never come to light through using a test pack.

Finally, test packs are procedural tests only. They do *not* verify directly the balances shown on the profit and loss account or on the balance sheet. They cannot do this as they in no way examine client data, being restricted to dummy test data.

Computer audit programs

These software retrieval packages used by the auditor are themselves computer programs. They are usually general purpose packages which can be used on a variety of different computers for a whole range of tasks which are specified by

means of parameter-oriented coding sheets filled in by the auditor. They can read files and extract defined information. They can prepare analyses and special reports. They can 'audit' files by conducting comparisons between different items of data (often held on more than one file), by checking data for reasonableness and by totalling selected fields. As with test packs these computer audit programs should only be used when conventional procedural tests or verification checks are inadequate. The sequence of steps the auditor should follow when he plans to use a computer audit program are:

1. Define the problem
2. Eliminate conventional means (e.g. a special printout using an existing client program)
3. Find a suitable computer audit package *or* specify and write a suitable program
4. Test exhaustively the package or program
5. Maintain physical control over the computer audit program
6. Maintain physical control over the file(s) processed (e.g. by obtaining a copy)
7. Obtain computer time
8. Attend the run.

While the auditor may never be found out (it is difficult to tell whether an auditor has done a good or bad audit) it is of course bad practice not to define the problem and identify precisely the job to be done by the audit program. Failure to do this once resulted in the balances of 200,000 customer accounts being printed out 25 to a page—almost two miles of continuous stationery, all quite useless as the auditor had forgotten to ask for subtotals on each page: as a consequence he was unable to tie in any of the balances shown for customers with the grand total which was shown at the end of the listing. He declined to admit his way through the listing!

It will be recognised that this powerful interrogation method is useful for verification work (as it analyses live data) as well as procedural testing (as it can check in retrospect that data has been processed correctly). It is also timesaving as it facilitates examination and analysis of data at electronic speeds. It is ideal for selecting either quota or random samples. While the capital investment in developing such a package is high it is now possible to purchase ready made packages and of course they are relatively permanent. They are flexible in function in that what the package does can be simply modified by means of parameters. They are not excessively expensive to run but of course they do require set-up time in addition to run time and once again a detailed knowledge of the client's computer system is required. Both the internal and the external auditor may use computer audit programs to save time for instance in the selection of samples even though in theory the audit trail would allow this to be done manually though tediously. This is not a misuse of audit programs: computers have always been used in place of clerks to do repetitive, routine tasks and they are generally-speaking quite cost effective in this area.

Real time systems

It was fortunate for the auditor that manual systems usually provided audit trail automatically by way of the hard copy that the system generated in order to function. By and large the auditor's problem was merely to ensure that the trail was retained for an adequate period. So the impression that audit trail was never forgotten in the old days is largely a happy illusion. Routine batch processing administrative computer systems also usually had adequate audit trail by default rather than design, for once again it was true that hard copy featured prominently in the system so that the system could work satisfactorily. This was not always the case and there have been many instances of audit controls being omitted by systems designers or tagged on as an afterthought rather than incorporated at the initial systems design stage.

As there has been a reaction against producing hard copy of everything the computer does it is necessary for the auditor to be particularly vigilant to ensure that he has the trail he (and often the company) really needs.

Everyone's output is someone's input: it is clearly inefficient to produce on computer listing paper information which then has to be coded, keypunched and read into another computer. It would be better if magnetic tapes of data were exchanged by computer users, viz. the example of credit transfers on magnetic tape being delivered by companies to banks. Better still, computers are technically able to converse with computers. We are therefore moving into an era when audit trail can no longer be expected to be present as a by-product. Rather there is a risk it will be bypassed. It is more important than ever before that the systems designer should build in audit controls into the systems he designs. The auditor for his part must be prepared to accept records held on media other than paper as adequate audit trail so long as they are 'in a reasonably accessible form'. This means that magnetic tapes or microfilm should suffice.

On-line and real time systems pose special problems. Real time systems are those where the response from the computer is *very quick indeed* and is quick enough to affect the *outcome of the transaction itself*. On-line systems do not imply these characteristics but simply that information relating to transactions is sent via a keying device down a line to a remote computer and sometimes vice-versa. With either type of system there is a grave risk of audit trail not existing unless it is specifically built into the system. The risk is greater in the case of real time systems where the requirement for immediate response

often implies no time and no immediate need to make out hard copy documentation. Auditors must re-examine their case for demanding records which companies feel they no longer need to operate effectively. From the company's viewpoint a loss of control may be justifiable if the cost of such a control is greater than the risk of the consequences of not having the control. The auditor should look for new methods wherever possible to avoid asking the company to incur costs exclusively on behalf of the auditor.

Both the techniques of test packs and of computer audit programs can be developed for real time systems. On a real time system for dispensing cash from an automatic machine outside a bank, the auditor's test pack may be a few dummy cash cards associated with a few dummy accounts held on the computer files at the remote location. The counterpart of the computer audit program may be a resident real-time program active whenever the real time system is active. This program would vet the disposition of incoming messages, accumulate statistics on terminal usage and the number of cancelled enquiries and so on, select samples to be printed out for action in the form of further testing by the auditor and scan the database to search out incompatibilities or other situations arising which could indicate that the system is out of control. With this sort of real time computer audit program it is arguable that the external auditor should never again insist on audit controls and audit trail unless it can be demonstrated that the company needs these controls for management purposes. It has already been shown that the internal auditor would never insist on controls beyond those which are essential to management for management purposes.

Dr S Gill

Journal readers will be shocked and saddened to hear of the death, at the early age of 49, of Stan Gill. He will be remembered especially as the author of the first paper to be published in the *Journal* (Parallel programming, Vol. 1, No. 1, p. 2) and as the Chairman of the Editorial Board until his death. A full obituary will appear in the June, 1975 issue of *Computer Bulletin*.