Computer Auditing

Computer Auditing

Third Edition

Andrew D Chambers BA FCA FCCA FBCS

Sub-Dean Administration and
BP Professor of Internal Auditing,
City University Business School

John M Court BA FCA MBCS

Secretary of the Information Technology Group
of the Institute of Chartered Accountants in
England and Wales

Pitman

Pitman Publishing
128 Long Acre, London WC2E 9AN

A Division of Longman Group UK Limited

First published in 1981
Second edition in 1986
Third edition in 1991

British Library Cataloguing in Publication Data

Chambers, Andrew D.
Computing auditing. – 3rd ed.
1. Auditing. Applications of computer systems
I. Title II Court, J. M. (John Michael) *1943–*
657.450285

ISBN 0 273 03241 0

Typeset, printed and bound in Great Britain

Preface to the Third Edition

The first edition of *Computer Auditing* was published at the end of the 1970s. This was the first age of computer auditing. We still used to say in those days 'all auditors will one day have to be computer auditors'.

The end of the 1980s saw the second edition. This was the second age of computer auditing — consolidating the theory and extending the practice so as to adopt the process of auditing to the near-universal business use of computer systems and to the continuing proliferation of microcomputers and personal computers throughout businesses of all sizes. We used to say that all auditors should by now in theory be computer auditors but that in practice there was still some way to go.

The 1990s takes us into the third age of computer auditing — the age of mature theory, recognised best practice and distinctive professional qualifications. The third edition of *Computer Auditing* — which incorporates an extensive rewrite of many sections, a large amount of new material and a major change in presentation — reflects the maturity of the state of the art. The book is primarily addressed to the auditor who is not a technical specialist — but who, being an auditor, needs to be a computer auditor. However, the text addresses the relevant technical issues to the necessary extent. No auditor, being a computer auditor, can avoid them, or should wish to do so. We can at last say that all auditors are indeed computer auditors — though some do still need to be more technically specialised than others.

This third edition reflects the increasing pace of implementation of information technology (IT). New material covers such subjects as:

- trends in IT and their impact on auditors:
- audit of forward planning;
- developments in networks, electronic data interchange and multi-user systems;
- automated auditing procedures;
- use of packages (either on their own or in conjunction with systems developed in-house);
- variety in methods of developing systems;
- users developing and implementing their own systems with limited (if any) recourse to technical specialists;
- legal developments.

We have also sought to include more material in the form of checklists and questionnaires. We believe that audit is, above all, a set of practical tasks rather than theoretical exercises.

In producing the third edition, we would like to renew our thanks to those who helped us to prepare the first two editions. Those to whom

acknowledgement are due include E. A. Evans, W. List, B Matthews and P. W. Morriss. We would also like to express our gratitude to Nicki Muggridge, who has helped us to research the implications of current technological developments, Furrokh Billimoria, Adrian Norman, David Saunders and Graeme Ward, who have also contributed greatly to our thinking, and David Lewington whose original ideas were the initial inspiration for Chapter 8 on risk analysis in computer auditing. Many thanks are also due to Margot Ellis who has processed most of the words in the book often by deciphering scrawled manuscript of the most remarkable obscurity.

We would also like to recognise our debt of gratitude to the Institute of Chartered Accountants in England and Wales, one of the world's leading professional bodies, to the work of which we have both been privileged to contribute for so long a time, as well as to those members of the staff and students of the City University Business School, London, who have helped in many ways.

Any faults and deficiencies in the book are of course entirely our own responsibility.

A.D.C.
J.M.C.
1991

Contents

Part 1

State of the Art

1 Overall Management Objectives — Overview

- Commercial computing
- Control objective

Commercial computing

Computer applications are widely used to support commercial activities, in both large- and small-scale business environments, and functionality depends largely on software. This is why both internal and external auditors are almost certain to become involved in the design or evaluation of such systems, the use of such systems in the course of their work and the implementation and checking of procedures adopted to ensure that the use of such systems is properly controlled.

For example, sales order entry and accounting systems are among the most promising applications. The idea is that the user keys in the details of an order, maybe at the moment it is received, and then the system generates the delivery note and invoice, updates the sales transaction records for the day and the customer's account in the sales ledger, and perhaps updates the relevant stock records in the process.

The invoice can then be delivered along with the goods, instead of having to be sent out afterwards. In this way it gets into the customer's system, and hopefully out again with the customer's payment, as quickly as possible.

The user should usually have to intervene at two subsequent stages, although of course errors may have to be corrected, or other adjustments made, at other times.

First, the user will need to input information when the goods have been delivered, and the receipted delivery note comes back from the customer (or when the customer collects the goods). It may be necessary to modify the transaction record, for example, because the wrong quantity was delivered, or part of the delivery was faulty, and issue or generate a credit note. (Systems differ in respect of how much is done.) If the system is integrated with a stock recording system, it is very important to ensure at this stage that, if resaleable goods are returned by a customer, then they are immediately re-entered in the stock records.

Secondly, intervention will be required in order to record the payment received from the customer after an order has been delivered. Again, at this stage, a credit note may need to be issued, or a discount generated.

The system should generate the relevant daily and periodical accounting reports, and will also produce customers' statements, debtors' analyses, and

in some cases management information about the frequency and categories of goods ordered.

All this is what an integrated sales order entry system can achieve. Indeed, this sort of thing is what is implied by calling a system 'integrated' — that it updates all the interrelated records simultaneously, without the need for further manual intervention.

Such a system should also be interactive. The user should be able to call back details of any transaction on to the screen, including full information about its current delivery and payment status, without any technical difficulty.

The user certainly has to be aware of some of the pitfalls of such a system — why it may not work well in practice. For example, some systems do not cope well with non-standard packaging or containers, if these have to be included in the amounts to be invoiced. Sometimes it is difficult to cater for more than the simplest type of discount calculations: differential discounts for different customers, or different periods of credit, may cause all sorts of complication. (This is an example of why it is difficult to evaluate software in isolation from the conditions of its use — it all depends in such a case on how flexible the user wants to be.)

Retailers, of course, do not normally need such systems. However, together with manufacturers and credit traders, they may be able to use the stock recording software with which order entry systems are often themselves integrated. One of the major features of good stock recording is the ability to stimulate reordering, purchasing or the need for production of stock lines as soon as a critically low stock level is reached, and indeed to discourage unnecessary reacquisition while stocks remain above this level. Good stock control is, of course, an important component in maintaining liquidity.

The system should produce an appropriate reorder listing. It must be able to differentiate between stocks which have been allocated for delivery, even though they are still held in the storeroom or warehouse or are in transit to customers, and stocks which have actually been delivered. Reorder levels are affected as soon as stocks have been allocated, not when they leave the premises, particularly if an invoice has already been produced by the system in respect of the sale.

The main pitfall is that unless the user is very conscientious in entering every single stock movement, in or out, the benefits of such a system will very quickly become counter-productive. The quantities recorded by the system, and compared with the reorder levels in order to generate the reorder listing, will be incorrect and the reorder listing will therefore be of no value. The effects of not being very accurate in record-keeping will be out of proportion to the number of individual mistakes. It will then be better not to use the system at all than to try to compensate for the incorrect management information which, through the users' own fault, the system will have generated. Or at least it will be better to make the effort to bring the records maintained by the system back into conformity with the real world.

The use of bar coding may be relevant to warehouse systems, to the

control of distribution and to more homely environments such as retail check-out counters. Whatever the case, bar code control facilitates the input of records of movements but does not necessarily overcome the problem of input error: the bar code still has to be read correctly (and once only) when a movement takes place.

One way of overcoming this possible problem, in a warehouse or in the case of wholesale distribution, is the use of a fully robotic stock movement system, such that the physical movements, carried out by the robots, are recorded by the system as they take place.

Stock order and movement systems, together with those which deal with sales, purchases and nominal ledger maintenance, are at the heart of computerised financial accounting procedures. Other computer systems, dealing with such matters as payroll computation, fixed asset accounting and share registration, are also often crucial in this connection.

The financial accounting function is very important. However, at least equally important, and in some ways often even more so, is the function of management control.

Control objective

Stated in general terms, the most important aspect of commercial data processing is, or at least should be, the production of accurate and useful management information to assist all levels of management within the business to maximise profit and minimise loss.

The major control objective of any business or other organisation is that management uses information of optimal value, in terms of timeliness, completeness, accuracy, consistency, clarity, conciseness, relevance, security and economy, in assisting them to meet their objectives.

This is the primary purpose of all support activity including computer auditing. All detailed support work should be planned and implemented with this overall objective in mind.

The questionnaire which follows is designed to assist in the fulfilment of this overall control objective. It does not deal directly with any specific aspect of computer processing, but provides a framework within which an auditor may make judgements about the relevance, applicability, relative priority and comparative resource justification of different audit techniques, with reference to the particular circumstances and conditions of the business or organisation being audited.

Key questions

1. General

(a) Has responsibility for management information been formally designated to a member of the management team?

(b) If 'Yes', does this person's brief include an appraisal of the following:
  (i) quality of management information?
  (ii) satisfactory utilisation of management information?
  (iii) continued appropriateness of management information in the light of changing political, legal, economic and technical circumstances?

(c) Are there adequate written procedures on the preparation and use of management information?
(d) Is management information originated at the correct sources?

2. Timeliness

(a) Are deadlines laid down for the preparation and distribution of management information?
(b) Is management information produced at the most appropriate intervals?
(c) Is management information based upon up-to-date data?
(d) Is management information produced promptly in accordance with laid-down deadlines?
(e) Is management information kept no longer than necessary? (For instance, out-of-date price lists are dangerous.)

3. Completeness

(a) Does the management information system enable management to ascertain the following:
  (i) that all important laid-down procedures have been complied with?
  (ii) the extent to which significant errors have occurred?
  (iii) the extent to which all control points have operated satisfactorily?
(b) Does the information system cover all aspects of the business?
(c) Is there a budgetary control system?
(d) Does the information system adequately cover the operational needs of managers?

4. Accuracy

(a) Is all management information based upon adequately reliable data with no practical ways of improving upon the reliability of the data?
(b) Are the data upon which the management information is produced, and the management information itself, checked as necessary for reliability?
(c) Is an appropriate balance struck between the often conflicting objectives of accuracy and timeliness?

5. Consistency

(a) Is there adequate consistency between each edition of periodic management reports?
(b) Are the data used as a basis for management reports mutually consistent — especially when drawn from different sources?

6. Clarity

(a) Are all management reports:
  (i) unambiguous?
  (ii) legible?
  (iii) attractive?
  (iv) clearly titled, dated and captioned?
(b) Is clarity achieved with respect to the presentation of figures which relate to each other:

(i) in comparison of the results of periods?
(ii) in comparison of 'actual' with 'budget'?
(iii) in comparison of cumulative data with prior cumulatives?

7. Conciseness

(a) Are all management reports as concise as possible without being too brief?
(b) Is full proper use made of reporting only by exception?

8. Relevance

(a) Is all management information relevant to:
(i) the business?
(ii) the responsibilities of those who receive it?
(b) Is the requirement for the information known to those receiving it, as well as to those preparing it?

9. Usefulness

(a) Is the information provided all capable of being acted upon?
(b) Does the information, actionable by those to whom it is provided:
(i) relate to the manager's span of control?
(ii) generally come within the manager's sphere of responsibility?
(c) Is management information acted upon by management;
(i) promptly?
(ii) appropriately?
(d) Are exceptions on exception reports all followed up?
(e) Are comparative figures provided where appropriate?

10. Security

(a) Are adequate arrangements in force and applied to provide satisfactory security over (A) the preparation, (B) the distribution, (C) the custody, and (D) the disposal of information, in order to preserve the requirements of confidentiality with respect to the following:
(i) the business?
(ii) employees?
(iii) third parties?
(b) Is there an inventory of information at risk?
(c) Are retention periods for information adequately correctly defined, and are they minimised commensurately with all necessary requirements for their retention?
(d) Is information securely disposed of?
(e) Is access to sensitive information restricted to defined personnel?
(f) Are all staff handling sensitive information (A) carefully selected, (B) fidelity bonded, and (C) closely controlled?
(g) Is the release of information (A) to insiders, and (B) to outsiders, properly authorised?
(h) Are there official channels for handling requests for sensitive information, and are these followed?

(i) Are all company secrets kept securely locked up?
(j) Is there adequate security over keys, including spare copies?
(k) Are there appropriate building access controls?

11. Economy

(a) Is all produced information necessary and none of it excessive?
(b) Is all information prepared with maximum economy (consistent with other requirements) with respect to:
  (i) collection of data?
  (ii) recording of data?
  (iii) processing of data?
  (iv) presentation of management information?
  (v) distribution of management information?
  (vi) custodianship of management information?
  (vii) utilisation of management information?
  (viii) disposal of management information?

2 Computer Auditing — Overview

- Audit processes and techniques
- Audit specialism
- Audit skills and experience

Audit processes and techniques

Chapter 1 illustrates how computer systems have come to pervade all aspects of commercial life. Comparable developments have occurred in organisations offering services rather than goods and in organisations dealing with public and private administration and the public service, so no auditor can ignore the effect of such developments.

'Computer auditing' — a term coined in the days when no one had really analysed what it meant, and when computer audit specialists were regarded as a curiosity — has many distinct components. First, auditors often use a computer to help them in their work. For example, they use file interrogation programs to select samples, to confirm totals and to reperform calculations. The first file interrogation package for auditors was launched in 1965. Many others have followed. They all, in one way or another, require the auditor to modify a pre-existing shell program so that it comes tuned to the requirements of a specific audit.

The simpler audit packages can be regarded as report generators. More complex and powerful audit software, however, functions as a program generator and resembles a high-level programming language in its own right. In this respect, audit packages foreshadowed the general query languages, 'fourth-generation languages' (4GLs) and fifth-generation ('expert') systems, all of which enable users to select and manipulate information on computer files without themselves having to be programmers or systems analysts. Computer auditors are often pioneers in the use of new techniques.

An auditor using a computer program (and it certainly does not necessarily have to be an audit package) may need to rely on the functions of the computer's system and its adjuncts such as database management software, network control systems or teleprocessing monitors. This may also be necessary if the auditor is seeking to prevent or detect fraud perpetrated through misuse of a computer. A few auditors therefore need to specialise in systems support techniques. Others need at least an ability to talk to systems support specialists in their own technical jargon — based on a sound level of technical knowledge.

Some auditors also use special procedures to test the continuing integrity

of computer systems. Certain techniques directly check the detailed instruction in a computer program. Other procedures use dummy data to test computer programs indirectly — by checking that they produce the expected results in a variety of different circumstances.

These techniques are all variants of those used to test computer systems while they are being developed. Current system development methodologies can be very sophisticated. For example, mathematical techniques can sometimes be used to prove that certain aspects of the programming are correct. Auditors who are going to test systems, or to audit the system development process, ought to be aware of the relevant techniques — but should also be aware that a program may be formally and structurally sound, yet still not do what its users think it does.

The details of the system development may not always be known — for example, if a micro-based accounting package is to be used. It is still very important for the potential user to test the operation of a package before it is acquired. The method of testing, however, may differ radically from that applicable to a system developed by the users themselves. It may be mainly based on the experience of existing users of the package or on evaluations by independent consultants. Auditors should be able to give advice on this and other sound procedures for testing and evaluating packages.

In many ways, however, 'computer auditing' is better described as simply 'auditing in a computer environment', with reference to the programmed controls carried out by computer applications (such as sales accounting or payroll) and the manual controls exercised by their users.

The relationship between the programmed and manual controls is important — for example the production of an 'exception report' based on the programmed detection of unusual data, is of no use unless it is examined and followed up clerically. Auditors must consider the controls over data input to and output from these applications and over data contained in the computer files and generated by the programs. These application controls are vital. The general controls over computer installations, micro-computers, terminals, files and programs are also important. A person may gain access to files and programs physically — a diskette or tape can be carried away — or from a terminal. Both types of access need to be controlled if the integrity of the computer system is to be maintained.

So auditors (in common with security guards) are interested in the physical protection of computers and file media and (in common with system support specialists and network support specialists) in the use of the operating system software to protect the files and programs. From both points of view, auditors need to consider whether adequate arrangements for back-up and disaster recover and insurance cover have been made.

Auditors often perform financial audits. But they may also be called upon to do special investigations, fraud detection, efficiency and 'value for money' audits and exercises to ensure conformity with standards and authorised procedures. These more specialised activities are often undertaken in connection with computer systems.

Different types of auditors emphasise different components of 'computer