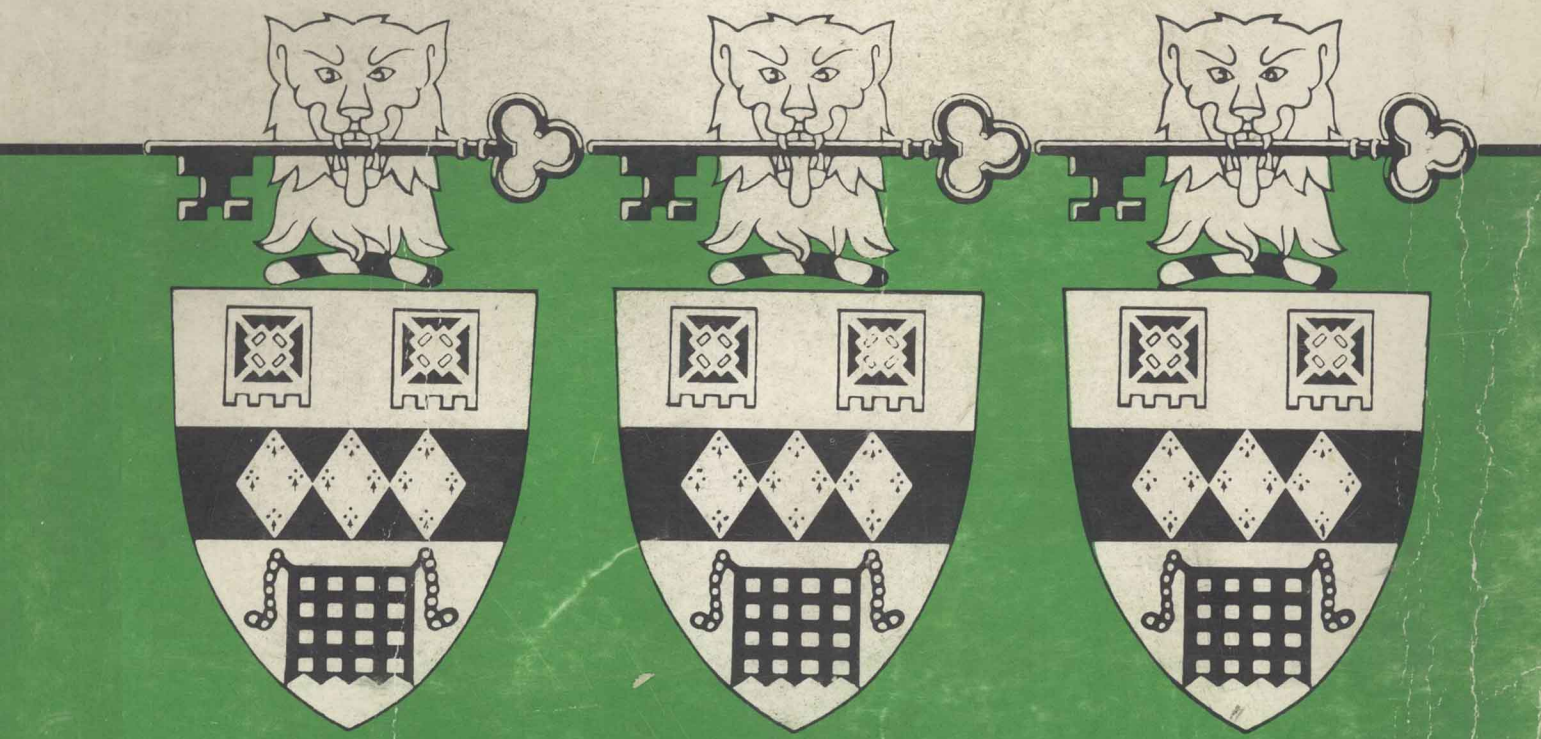
AUDIT AND CONTROL OF DATABASE SYSTEMS

THE BRITISH COMPUTER SOCIETY



THE BRITISH COMPUTER SOCIETY

'AUDITING BY COMPUTER' SPECIALIST GROUP

AUDIT AND CONTROL OF DATABASE SYSTEMS

JULY, 1977

AUDIT AND CONTROL OF DATABASE SYSTEMS

FOREWORD

This publication has been prepared as a result of studies undertaken by three separate sub-groups of the "Auditing by Computer" Specialist Group of the British Computer Society. The three sub-groups concerned - City, Westminster and Kingston groups, each produced a paper reflecting the experience of the members in that group with database applications. The experience of these three groups is complementry; the City group largely represented the interests of the external auditor whilst the Westminster group was largely experienced in the central and local government sphere; the Kingston group had a considerable academic element. Nevertheless, the views put forward by the three groups overlap extensively but each group's contribution has been included in the publication as an individual paper because it is felt that the differing approaches to the various problems may clarify for some readers the more technical concepts involved.

In general terms the Specialist Group does not see the audit of a database system as being fundamentally different, either in structure or approach, from that of any other computer system. The papers included in this publication largely assume the existence of a suitable EDP audit function, be it internal, external or both, to carry out successfully the audit of a conventional computer based system. The papers therefore limit discussion to the characteristics peculiar to a financial database system and to the changes in organisation and techniques which result. Naturally all three study groups became involved to a limited extent in considerations affecting the implications of transaction based terminal operations which are usually associated with the operation of a database system.

Although database technology has been around now for several years it is only in the last few years that organisations have developed database systems involving financial data; experience and standards in the field of controlling such database applications are still limited. One of the principal objectives of producing this publication was to provide a basis for further discussion on the topic of controlling and auditing database systems and neither British

Computer Society nor the individual study groups who have produced these discussion papers would profess to claim that these provide a comprehensive solution to what is a very complex problem.

At the front of this publication there is an index which you may find helpful should you wish to locate the information and various recommendations relating to such questions as 'when should auditors get involved?' or 'can audit software access database files?'.

As already indicated, this a discussion paper; should you wish to obtain further information regarding a particular aspect included in any of the three papers or you would like to put a point of view to the Specialist Group you should do so by contacting the Secretary of the Auditing by Computer Specialist Group.

This publication has been produced by the Auditing by Computer Specialist Group of the British Computer Society. The views and opinions expressed in this publication are the personal views and opinions of the authors and not necessarily those of the organisations whom they represent or of The British Computer Society.

F.E. HINCHCLIFF
Chairman,
'Auditing by Computer'
Specialist Group
The British Computer Society
21st July 1977

THE BRITISH COMPUTER SOCIETY

AUDITING BY COMPUTER SPECIALIST GROUP

MEMBERS WHO CONTRIBUTED TO THE PREPARATION OF THIS PUBLICATION.

DATABASE STUDY GROUPS COMMITTEE

A.I. Edmonds - District Audit Service (Leader - Westminster Study Group)

F.E. Hinchcliff - Hambros Bank Limited (Chairman - Auditing by Computer Specialist Group)

W. List - Thomson McLintock & Co (Leader - City of London Study Group)

J.M. Ross - Peat, Marwick, Mitchell & Co (Secretary - Auditing by Computer Specialist Group)

A.J. Thomas - Kingston Polytechnic (Leader - Kingston Study Group)

STUDY GROUP MEMBERS

CITY OF LONDON

D.C. Cale - Coopers & Lybrand
S.A. Carter - Price Waterhouse & Co
W.J. Cooper Bailey - Peat Marwick Mitchell & Co
J.M. Court - Whinney Murray & Co
C.G. Forsdyke - Bankers Trust Company
M.J. Gadsden - Touche Ross & Co
Mrs H.J. Godfree - Bank of England
R. Palmer - Farrow Middleton & Co

WESTMINSTER

R.S. Lay - London Borough of Haringey
A.S. Matthews -)
I. Robertson -) Central Computer Agency
D.M. Rose -)
D.E.J. Wilson - IBM (UK) Limited.

KINGSTON

D. Frost - Mann Judd & Co
J.L. Harris - Data Processing Centre, Kingston Polytechnic
Miss R. Pattisson - Hambros Bank Limited
D. Rohan -)
D.P. Ruback -) Josolyne Layton Bennett & Co
N. Sheldon -)
P.G. Stebbings - Mann Judd & Co

AUDIT AND CONTROL OF DATABASE SYSTEMS

INDEX

SUBJECT MATTER	Page/Paragraph References		
	CITY	WESTMINSTER	KINGSTON
General security, backup, recovery	30/88-89	76/5.5	91/2.1.2 127/4.4 137/4.8 148/4.12 152/4.14
Monitoring and testing the database	28/74-79	73/4.6 76/5.4.2 77/5.6	104/3.5.5 110/3.7 140/4.9-4.11
AUDIT OF A DATABASE SYSTEM			
Impact of database on the Audit	9/15-22 35/99-105 42/123-127	49/1.2 74/5.1	88/1.3 157/5.1
Specialist Training/technical requirements for auditors	41/120-122	62/4.1	114/4.1
Timing of audit involvement	36/104-105	74/5.1	157/5.1
Areas requiring involvement	37/106	53/3.2	89/1.3.2 157/5.1-5.7
Nature of involvement	38/109	53/3.2	91/2.1 157/5.1-5.7
Audit trail	-	-	123/4.3
Use of test data	39/111	62/4.1 73/4.6	159/5.3
Use of software for audit	39/112-119	71/4.4 76/5.4.3	115/4.1(e) 134/4.5 162/5.7

AUDIT AND CONTROL OF

DATABASE SYSTEMS

CITY STUDY GROUP

of the

AUDITING BY COMPUTER SPECIALIST

GROUP of THE BRITISH COMPUTER SOCIETY

INDEX

FOREWORD

1 This report has been prepared by the city study group of the British Computer Society Audit By Computer Group after its consideration of the audit and control problems associated with database file organisations.

2 The members of the study group were:

W List	-	Thomson McLintock & Co - Leader
J M Court	-	Whinney Murray & Co
M J Gadsden	-	Touche Ross & Co
D C Cale	-	Coopers & Lybrand
Mrs H J Godfree	-	Bank of England
C G Forsdyke	-	Bankers Trust Company
W J Cooper-Bailey	-	Peat Marwick Mitchell & Co
R Palmer	-	Farrow Middleton & Co
S A Carter	-	Price Waterhouse & Co

3 The views expressed in this report are an amalgam of the ideas of the members of the study group but this does not imply that any individual member of the study group supports all the ideas put forward. The group wish it to be viewed as a contribution to the continuing debate on the optimum methods of control of applications using database file organisations.

Limitation of this report

4 The study group considered the implication of database file organisation upon the maintenance of an organisation's records, particularly financial records. We fully appreciate that different criteria may be applicable to the processing of other types of application (eg computerised flight control for aeroplanes) but these were outside the scope of the group's remit.

5 The group has been constrained in its comments by the scarcity of fully operational databases in the UK within commercial undertakings. There are a number of database applications in various stages of development but as yet few have approached the size or complexity advocated in theoretical articles on databases. To this extent therefore the full impact of the radical change in the construction of an organisation's records has yet to become apparent to the majority of management and staff with whom the group is in contact.

Control principles for computer applications

6 Over the past ten years there have been a large number of books and articles published which enunciate and explain the control principles and techniques applicable to computer systems. In addition, universities, the accounting institutes, computer manufacturers and others have run a very large number of courses which explain these principles and techniques to participants. The group consider that these basic principles still apply although the techniques necessary to implement these principles will change.

7 The experience of the group is that whilst the principles of control are basically understood, the degree of rigorous enforcement of procedures to apply these principles leaves much to be desired at present. It is the unanimous belief of the group that the enforcement of control procedures must improve markedly if commercial databases are to be effectively controlled.

8 This report is an attempt to isolate the areas of change brought about by the introduction of database technology and therefore does not cover any areas which we believe to be unchanged. The group wish to emphasise that this is not because we consider them unimportant but simply that they are not germane to this report.

The structure of the report

9 The group believe that it is the responsibility of the management of an organisation to define and enforce the necessary procedures to process its records correctly. It is the auditor's duty to check the records and the procedures whereby management ensure that they are correct. The report is divided into five sections:

a What is a database and our concerns?
b The structure of the user organisation.
c The requirements of user department line management.
d The procedures required in the data processing department.
e Audit considerations.

We particularly differentiated those matters which we believe to be the responsibility of management (sections b, c and d) from those which are the responsibility of auditors (section e). This is not in any way intended to limit the role of auditors or consultants in assisting management in performing its duties but more to draw a clear distinction between the two roles.

WHAT IS A DATABASE AND OUR CONCERNS

Introduction

10 In this section of the report we set out our definition of a database, and the matters which we believe give rise for concern by both management and auditors.

Our definition of a database

11 A database in the context of our report is a method of storing data which has at least the following attributes:

a It must contain all relevant data - in the ultimate all the organisation's data.

b The organisation of the data on magnetic devices is independent of the logical records required by application programs.

c In addition to the data the means of locating the data on the magnetic devices must also be stored.

The database management system

12 In order for application programs to gain access to the data within the database instructions by the application programs are issued to a suite of programs which maintain the database itself (called a database management system - DBMS). In addition to maintaining the database structure DBMS suites also:

a provide facilities to prohibit access to data by application programs,

b present to the application program only those data items requested by the program,

c provide facilities for creating logs of events affecting the database.

d provide utilities to reorganise the data.

Two objectives of a database

a Data items will be stored once

13 In the past particular items of data have been stored on a number of different computer files or a number of times on the same file. This has given rise to the problem of ensuring that at all times the same data item has the same value within the computer system(s). It has become a fundamental principle of the implementation of databases that the number of times that a data item is stored should, as far as possible, be reduced to one.

b Programming flexibility

14 In the past it has been necessary to define the format and storage characteristics of the data within each program. This has meant that each time either the format or storage characteristics of data have been changed it has been necessary to amend the programs which access the data. In a database the physical storage of the data and the means of accessing that data are independent of the application programs therefore it is unnecessary to amend every application program when data characteristics are changed. Naturally if additional items of data are to be stored on a database then those programs which require to use the data will require amendment, but not those which do not need to use the data. By this means greater long-term program reliability will be achieved which will assist in limiting the possibility of errors.

Why we, as auditors, are concerned

a The definition of data

15 In order to achieve the objective of storing each data item only once, it is fundamental to ensure that there exists a consistent and accurate definition of what each data item is. Within large organisations we believe that this may prove difficult to achieve because data items are known by departmental jargon which may inhibit the clear understanding of what data items really are.

b Data relationships

16 As an item of data is stored once it follows that all users of that item of data will always access the same item. It is therefore important to ensure, as far as possible, that each item of data is always 100% correct. In this context 'correct' implies both absolute correctness and also correctness in relation to all other items of data within the database at the time of use. We are however concerned that as the scope of the database increases the number of relationships which a specific data item bears to other data items will become very large. It is therefore likely to prove difficult both to define these relationships accurately enough and having defined them to ensure that each data item conforms to them at all times. If this is not achieved, then the reports produced by computer applications using the database will, or may, be providing the management and the auditors with inaccurate information.

c Concentration of functions within the data processing department

17 The maintenance of the DBMS suite of programs and the physical organisation of data on the database are duties which can only be discharged by members of the data processing staff who have specialised knowledge and experience. Such staff are referred to in the technical literature as the 'database administrator' (DBA). It is likely that, at least in the early stages of development, the DBA team will be small in relation to the total data processing staff.

18 Clearly, the dependence of an installation on a small number of staff who are criticial to processing raises the question of the ability to continue to maintain proper records in the future, if for example all members are ill for a long period.

19 The group fully appreciate that within a computer system all things are possible provided one has the technical skill. The group is particularly concerned that the DBA team will, in the course of its normal duties, have legitimate access to the totality of the DBMS - the majority of the program and systems documentation (in order to assist in debugging any errors which have occurred) and to the data within the database itself. It seems to us therefore that this provides the DBA team, who already have sufficient technical knowledge, with the access and opportunity to enable them to make unauthorised adjustments to both the DBMS and the data.

20 The group therefore believe that the totality of the control and security procedures built into a system using a database must be capable of detecting fraud or error committed by the DBA team. It may be impossible to design procedures capable of doing this whilst still ensuring that the DBA team have sufficient knowledge to perform their duties effectively. This is therefore an area to which the management and the auditors must pay particular attention.

d Management involvement in system design

21 The manual processing systems in an organisation evolved over a substantial period of time, rather being planned as a totality. The introduction of traditional computer systems caused considerable disruption to the historic processing patterns in manual systems. The extent to which the senior management in organisations felt able, or had the time, to become involved in the thought necessary to construct effective traditional computer systems is perhaps, with hindsight, seen to have been inadequate. If organisations are proposing to implement large scale database systems the resulting change to both the organisation's procedures and its processing methods will, in our view, be radical. To accomplish a smooth transition to the new methods and ensure that at all times the information provided to the management is sufficient for them discharge their duties adequately will require active participation by the senior management. We are concerned that senior management's other duties will not permit sufficient time to be devoted to this essential planning.

e Controls

22 There have been, and regretably still are, far too many computer applications which are created without proper consideration being given to designing procedures whereby the users can ensure that the totality of the system has performed adequately. It appears to the group that insufficient attention has been paid to this crucial area in the published literature. The study group is fully aware that at this early stage in the development of databases this is probably natural but is concerned that consideration will be left so late that there will not be effective procedures devised when applications go live using databases. We believe that failure in this area will lead to disaster for the organisation as it has in the past with traditional systems.