ISSN 0961-9358

casg
Computer Audit
Specialist Group

JOURNAL

VOLUME 3 NUMBER 3 WINTER 92

The British
Computer
Society

Members' Meetings for 1993

1993 January 13th (3.30 for 4pm) Royal Institute of Public Health and Hygiene	**Joint meeting with IIA-UK Home Counties** **Controlling IT**	Rob Melville City University Business School Leslie Willcocks Templeton College, Oxford
February 9th (2 to 5pm)	**Mainframe to micro security** **– talk with demonstration**	Bob Stuart Computer Associates
February 23rd (full day)	**Discussion Group** **Computer Insecurity**	Topic and speakers to be announced
March 9th venue to be announced	**Joint meeting with EDPAA London chapter** **Annual debate**	Speakers to be announced
April 13th	**UNIX network security**	Greg O'Shea KPMG Management Consulting
May 12th (full day) London International Press Centre	**Annual Conference** **Systems Integrity** **followed by the Annual General Meeting**	Speakers to be announced

Meetings are usually held at the Royal Institute of Public Health & Hygiene, 28 Portland Place, London W1N 4DE (Ground floor, Lecture Room 1), except as noted above. For last minute confirmation, telephone 071-580 2731 or 071-636 1208. Meetings start at 4.00 for 4.30pm, unless otherwise stated. Tea and coffee are available before each meeting; sandwiches and refreshments afterwards.

Details of discussions groups are forwarded directly to members as part of the quarterly mailing. Please contact Chris Birt on 071-790 0755, or Steve Pooley on 0580-891036, for further information.

For details of the annual conference please contact Ian Longbon on 071-220 8495 or Paul Howitt on 0992 27923.

IN THIS ISSUE

- **DB2 Applications**
- **EDI Security and Audit**
- **Audits on IBM AS/400**

Editorial

From an editorial point of view, this has been an excellent year. A good supply of interesting and useful articles, not too many missed deadlines, useful feedback and a very professional production team is an editor's dream. There is even a waiting list of articles ready for future editions. It has to be said that in almost every other way 1992 will not be missed at all: redundancies, business failures, war and famine on a world wide scale. It's hard to be too optimistic in this sort of climate, but in many ways next year could prove extremely interesting for those of us who audit and control computers. With the constant pressure on costs which is likely to stay with us for a very long time yet, our skills in controlling and measuring systems come into their own. Unfortunately, there have been too many cases of shortsighted management who are so trapped by their narrowness of vision that they reduce and even make redundant their audit departments. This cannot be good policy, even if there is a short term benefit. John Mitchell's column alludes to potential inefficiencies in projects where managers decide to cut 'overhead' costs like audit. The very idea that a structured development methodology like SSADM can ensure that controls and effectiveness are built into systems is quite breathtakingly stupid. Just because rules and guidleines exist does not mean that they will be followed; if you think this is to overstate the case, consider the 'Ten Commandments' (the management summary derived from the system specification known as the Bible . . .)

• • •

Last month I attended another of the IEE seminars at Savoy Place. I have written about the excellent value of these before, and no doubt will again. For a very useful day of presentations and discussion, in a comfortable environment they are beaten on price and value only by our own meetings! The session was about prototyping systems developments, full marks to all speakers for their high quality presentations. Afterwards, it planted all kinds of fears in my head. Principally, it took the audit profession at least a decade to convice ourselves and our management that auditors could and should be involved in developing systems. Indeed the topic still appears in the Computer Audit examinations of the IIA. Secondly, if management can be shortsighted about the value of audit in bureaucratically controlled methodologies such as SSADM, how are they going to cope with incremental deliveries? Any papers on this topic will be welcomed.

• • •

It was at the Prototyping seminar that I heard a wonderful piece of computer speak: 'you knock on a coffin lid and out comes a C programmer'. Any C programmer who knows a funny story about computer auditors will be given every chance to respond in kind.

• • •

Thanks are due to all contributors, Janet at Carliam Typesetters, John Mitchell for being such an encouraging Chair, the Committee for organizing everything so well, my two students who pack the Journal into envelopes, the printers at City, and last but not least, the readers for making it all possible. Have a very happy holiday and let's hope the green shoots of recovery last longer than Norman Lamont's credit rating.

ROB MELVILLE

casg

Management Committee

CHAIRMAN	John Mitchell	Little Heath Services	0707 54040
SECRETARY	Ragu Iyer	KPMG Peat Marwick McLintock	071 236 8000
TREASURER	Fred Thomas	Retired Consultant	0371 875457
PUBLICATIONS	Jacqui Race	National Westminster Bank	071 860 4087
MONTHLY MEETINGS	John Bevan	Audit and Computer Security Services	0992 582439
	Alison Webb	Alison Webb Associates	0223 461316
CONFERENCE ORGANISERS	Ian Longbon	CWB Limited	071 220 8495
	Paul Howitt	Tesco Stores Ltd	0992 27922
DISCUSSION GROUPS	Chris Birt	Independent Consultant	071 790 0755
	Steve Pooley	British Petroleum	0580 891036
MARKETING & PR	Jarlath Bracken	Zurich Insurance	0705 822200
MEMBERSHIP SECRETARY	Jacqui Race	National Westminster Bank	071 860 4087
PLANNING	Bill Barton	The Rank Organisation Plc	071 706 1111
JOURNAL EDITOR	Rob Melville	City University Business School	071 477 8646

Contents

Chairman's Corner

John Mitchell

It's nice to see how this Journal gets around. Reading the *'Chad'* column in *'Computer Weekly'* a few months ago I noticed that they had picked up and used something from this very column. It's nice to know that our readership extends beyond the computer audit fraternity, as indeed does our membership. The move towards quality systems and TickIT now means that many other professions are taking an interest in the control aspects of I.T. Now if only we can persuade top management to take an interest as well . . . .

* * * * *

The London Ambulance System (LAS) fiasco once again raises the question as to whether the lessons from previous implementations are ever taken note of, or if we computer auditors are listened to early enough. I don't know enough about the LAS implementation to know whether, or not, there was Audit involvement during the development process (perhaps someone out there could let me know?), but once again I will 'sound off' on my favourite topic. It is our responsibility, nay our duty, as the control experts to stick our noses into any major development at a very early stage and make a constructive nuisance of ourselves. I have never subscribed to the 'it takes away our independence' cry of the weak audit department. We are there to help the organisation and by Jove, that's exactly what we should be doing, whether they like it or not!

* * * * *

I see that the long running Salvage Association versus CAP saga has finally come to a close with the Salvage Association being awarded damages and costs. Now if only the Association had employed a computer auditor to keep an eye on the development, they may have been able to avoid the need for long and costly litigation. Okay, this time they won, but a financial settlement still does not provide you with the system that you wanted and the litigation ties up your top management for a couple of years, when they could be doing more useful things.

I am often amazed at the short-sightedness of management when the budget for a proposed system is being prepared. Audit involvement should be included as part of the development cost, but often it isn't. I also remember one multi-million pound development, where I modestly submitted a proposal for £20,000 worth of audit involvement (after all I am a free-lance auditor), but was laughed out of court on the grounds of it being an unnecessary expense as they were using SSADM. They are still trying to make it work, some two years after implementation!

* * * * *

On a final note, I notice from Arthur C Clarke's biography (Sci Fi writer and father of the geostationary communications satellite) that his first job was as a clerk in a Whitehall auditing department in London. In view of his subsequent writings, including of course '2001 – A Space Odyssey', it brings a new meaning to the old adage "have auditor, will travel".

The compliments of the season and a prosperous and well controlled new year.

Guidelines for Potential Authors

In future, there will be two types of article in the Journal, refereed and invited.

Refereed articles should be technically oriented, and based on current or future issues related to computer audit, security or control. This type of article will be reviewed by at least one member of the editorial panel (anonymously). If published, it will be identified as a refereed paper.

Invited articles need not be purely technical, or overly academic (even Computer Auditors have a sense of humour!). This type of article will be reviewed only by the editor; this may lead to severe sub-editing, but submission will virtually guarantee publication.

We also invite members to volunteer for book, product and course reviews (anonymously if required).

Why not call Rob Melville at CUBS (071 477 8646) to discuss how you can get your name in print?

Audit Trail for DB2 Applications

Robert Gryg
Grafton Database Consultants Ltd
081 547 3440

Introduction

Over the last few years, many corporations have moved to a database strategy based on IBM's strategic database management system DB2. The relational database architecture of DB2, where data is held in table structures and is easily manipulated using the powerful structured query language facilities has resulted in a growth of new business applications.

Data held in the DB2 environment may be accessed and manipulated from connections established between several operating environments concurrently. The controls on access security are maintained using a combination of the internal security facilities of DB2 itself together with those facilities provided by an external security manager such as RACF or ACF2.

Once an application process has passed through the security interfaces, it is free to add, modify or delete data held within the DB2 environment. DB2 however, provides no automated audit trail showing the complete history of data changes made by these application processes to DB2 data (see Fig 1).

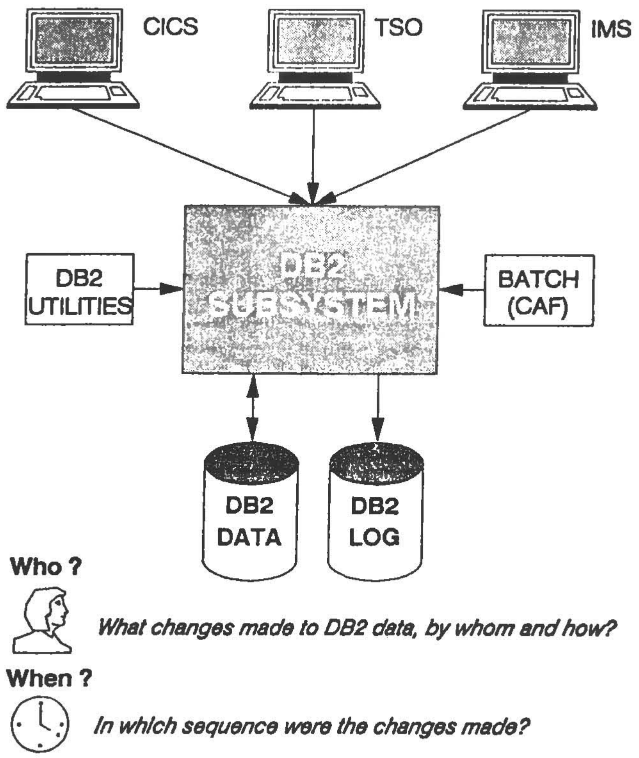

CICS
TSO
IMS
DB2 UTILITIES
DB2 SUBSYSTEM
BATCH (CAF)
DB2 DATA
DB2 LOG
Who ?
What changes made to DB2 data, by whom and how?
When ?
In which sequence were the changes made?

Fig 1. Multiple Connections to DB2

DB2 does provide an audit trace facility but its use is very limited as it shows only the request for a change and does not record any details of the change itself.

This paper introduces the facilities of the DB2/AUDIT software which has been specifically developed to enable a comprehensive system wide audit trail of changes made by application processes to data held in DB2 tables.

Using the DB2 Log for Audit Trail

Whenever a change is made to a row in a DB2 table, DB2 will record in its DB2 log, details of the row before the change was made and the details of the change itself. The change information recorded in the DB2 log is the minimum required by DB2 to support full recovery of the DB2 data.

When a row is inserted into or deleted from a DB2 table, the DB2 log will contain the full row image of the change. However, when a row is updated, the DB2 log will only show the contents of the row from the position of the update to the end of the row.

The DB2/Audit software is designed to read the DB2 log and for user selected 'Audited' tables, extract the relevant log records and construct an audit trail showing the full contents of inserted, deleted and modified rows. The audit trail is held in 'Audit' tables which as DB2 tables themselves, may be accessed using any SQL reporting interface (see Fig 2).

Audit Table Contents

For each DB2 table to be audited, a corresponding Audit table must be created. Each row in the Audit table will contain audit controls and a full row image of the row inserted, deleted or modified.

The audit controls show the date and time of the change, the type of change (insert, update-before-image, update-after-image, delete, etc.), the initiator of the change and the process through which the change was made.

The illustration in Fig 3 shows an example of the contents of an Audit table following the processing of six banking transactions:

1) A new account is created and a deposit made of £20. The account is given an agreed overdraft facility of £100. The 'I' row is inserted into the Audit table.

2) A deposit is made of £50. The Update Before 'UB' and Update After 'UA' rows show the full change history.

3) A withdrawal is made of £45. Again the 'UB' and 'UA' rows show the change history.

4) A rogue transaction adjusts the agreed overdraft facility from £100 to £250. Again the 'UB' and 'UA' rows show the change history.

5) A withdrawal is made of £275 and the overdraft facility is reset to £100. Again the 'UB' and 'UA' rows show the change history.

6) Finally, the account is closed. The deleted 'D' row is inserted into the Audit table.

An analysis of the history of these changes is available by using SQL as shown in Fig 4.

This example illustrates how the audit trail data can be used to identify how data inconsistencies could have occurred, as well as showing the movement of money through the system.

The analysis of the audit controls can also be used to show if userids holding high DB2 authorisation privileges, such as SYSADM, have changed sensitive data.

Operational Considerations

Until now, the requirements for audit trail will have had to have been built into the DB2 application itself. This approach has several limitations in that it involves additional development and maintenance effort, it adds to the performance cost of the application and most significantly, it does not highlight changes to the data made by non-application routes such as DB2 utilities or DB2 Interactive.

With the DB2/Audit software, the audit trail is guaranteed to be system wide without the need to modify existing or new applications. Furthermore, the audit trail can be limited to sensitive DB2 tables and collected on a frequency to suit operational requirements. For most users, the audit trail would be collected on an overnight basis enabling Audit Services to analyse all update activity of the previous day's online and batch processing functions.

Users of DB2/Audit

The principal users of the audit trail will be Audit Services although it may also be used to satisfy other application requirements. By using SQL based End User computing tools, the audit trail database can be interrogated to enable restruction of a complete history of changes to business data (financial and non-financial) and provide 'ad-hoc' reports.

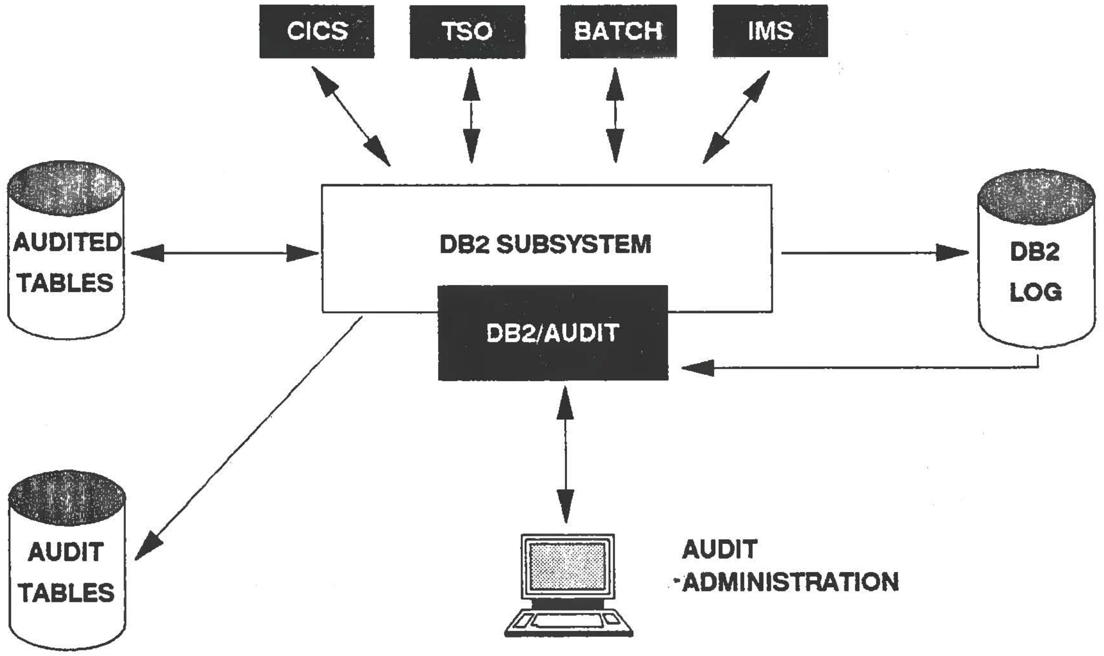


Fig 2. DB2/Audit Administration

◄ AUDIT CONTROLS ►◄ APPLICATION CHANGES ►

	▨	CHNG_TYPE_ID	▨	ACCT_NO	ACCT_BAL	LAST_TR_VAL	ACCT_OD
(1)	▨	I	▨	0012796	+20.00	+20.00	-100.00
(2)	▨	UB	▨	0012796	+20.00	+20.00	-100.00
(2)	▨	UA	▨	0012796	+70.00	+50.00	-100.00
(3)	▨	UB	▨	0012796	+70.00	+50.00	-100.00
(3)	▨	UA	▨	0012796	+25.00	-45.00	-100.00
(4)	▨	UB	▨	0012796	+25.00	-45.00	-100.00
(4)	▨	UA	▨	0012796	+25.00	-45.00	-250.00
(5)	▨	UB	▨	0012796	+25.00	-45.00	-250.00
(5)	▨	UA	▨	0012796	-250.00	-275.00	-100.00
(6)	▨	D	▨	0012796	-250.00	-275.00	-100.00

Fig 3. Audit Table Contents

```
    SELECT  CHNG_DTE, CHNG_TM, CHNG_TYPE_ID, USER_ID, PROC_NAME,
            ACCT_NO, ACCT_BAL, LAST_TR_VAL, ACCT_OD
      FROM  AUD_ACCOUNTS
     WHERE  ACCT_NO = '0012796'
       AND  CHNG_TYPE_ID IN ('I', 'UA', 'D')
  ORDER BY  LOG_RBA
```

▨	I	▨	0012796	+20.00	+20.00	-100.00
▨	UA	▨	0012796	+70.00	+50.00	-100.00
▨	UA	▨	0012796	+25.00	-45.00	-100.00
▨	UA	▨	0012796	+25.00	-45.00	-250.00
▨	UA	▨	0012796	-250.00	-275.00	-100.00
▨	D	▨	0012796	-250.00	-275.00	-100.00

Fig 4. Audit Table Analysis

EDI Security and Audit

(Synopsis of a talk)

by

W. List CA FBCS
The Kingswell Partnership
Harwell Laboratories, B166
Oxfordshire OX11 0RA
Tel 0235 820366
Int +44 235 820366

Introduction

Auditing EDI can mean many different things to different people, this is particularly so across international boundaries. Natural languages, traditions and customs in different countries and the increasing desire to define words very exactly all contribute to potential misunderstandings. Initially, therefore, I set out what I understand as an audit and identify the two main types of auditor.

Secondly I identify the types of contract within an EDI system and the UK record keeping arrangements relating to EDI transactions. Then I identify the types of audit that may exist in this environment and identify the key procedures that are likely to be subject to the audit(s).

Audit

An audit is the examination of an activity or formal document and the expression of an opinion on the quality of performance of the activity, conducted by people who are independent of the staff responsible for the performance and supervision of the activity. It is usual to include an audit report recommendation for the improvement of policies and procedures, including controls, where weaknesses are disclosed by the audit.

Auditors

There are two main types of Auditor: Internal and External. Internal auditors are employed by an organisation and perform work under the direction of the management of that organisation. There is a wide variation in the specific terms of reference for Internal Audit between organisations.

External auditors perform their work in conformity to statutory obligations. Traditionally this work has been conducted by individuals or firms with accountancy qualifications and has involved expressing an opinion on financial statements published by organisations. More recently governments have introduced requirements for external auditors to express an opinion on the systems being operated by (some types) of organisation. In addition external auditors perform specific contracted work at the direction of the management of organisations outwith their statutory duties. Certain organisations also employ consultants to perform technical audits particularly of computer systems and the security thereof.

In addition taxation authorities are usually empowered to conduct audits or inspections of organisations' records to determine if tax has been properly accounted for. In certain countries (eg UK) the authorities also have the power to prohibit the use of systems which they have not approved in advance.

The EDI environment

Within an EDI environment there are two main parties: the users of the service and the providers of the service. The service is a Value Added and Data Service (VADS). In addition, particularly in financial EDI systems (eg SWIFT), there may be suppliers of specific hardware and software necessary to operate the service. Certain EDI systems also include Certification centres, which certify users' public key(s) and/or Notorisation centres, which notorise individuals and/or specific messages. In this lecture I will treat these two types of centre as a specialised form of VADS.

These parties establish their relationship with each other through a series of contracts; these I will refer to as service contracts. These are to be differentiated from the contracts established between users of the service for the performance of commercial activity – possibly based on the Uniform rules of conduct for interchange of trade data by teletransmission (UNCID) issued by the International Chambers of Commerce. In this paper I will not consider the contracts for performance of commercial activity.

In certain cases the contracts between users impose obligations on the parties regarding the security and/or record keeping relating to their commercial activity. Clearly these obligations will be required to be considered in the conduct of an audit in the users' organisation.

EDI is used for international trade and therefore the procedures used, contracts established etc will require to take into account the variety of customs, traditions and legal and fiscal framework throughout the world. All countries and international bodies are seeking to amend the law and administrative procedures to incorporate the effects of automation. For example UNCITRAL is presently discussing matters relating to EDI as is the EC – TEDIS. Various reports have been prepared proposing amendments to international and national laws relating to unauthorised access to a computer. In addition differing regulatory frameworks exist within which VADS suppliers operate in different countries. These variations and the changes taking place make creating effective EDI systems on a global basis much more difficult than purely national EDIs.

The service contracts

As EDI is an optional activity the fundamental documents deferring the service are the service contracts. Any audit in an EDI environment must use these contracts as a starting point. Appendix I sets out in broad terms the areas covered by such contracts.

Of particular relevance to any audit activity are the provisions included in service contracts or interchange agreements covering:
security obligations, audit access to data, confidentiality requirements, limitation of liability for errors and failures, and record keeping obligations.

Record keeping

Over and above the normal commercial imperative of keeping adequate records, certain requirements are imposed by law and the ever more regulatory style of life (which I describe as quasi-legal).

These requirements fall into two broad classes:

- requirements to disclose information to the public or authorised bodies, which consequently causes a need to maintain the requisite details (but not necessarily on a computer);
- requirements to keep records of the organisation's transactions which often also specify the length of time such records should be kept.

Appendix II contains a brief summary of the UK sources of legal and quasi-legal record keeping requirements; similar provisions exist in other countries but some have specific requirements relating to computer records.

One overriding constraint on all the regulations is that the majority of requirements were originally framed before it became commonplace to use electronic equipment. Although amendments to the law or regulations are continually being made, the resulting rules never seem to be up-to-date with new methods of maintaining records. This is particularly true when addressing the needs in an EDI, paperless system.

In an EDI system there are two types of data; the commercial transaction itself and the details relating to the transmission and processing of that transaction.

Commercial transactions

In general terms all transactions of a financial nature need to be kept for a minimum of 15 months and a maximum of 7 years. Whether these are maintained on magnetic media/optical disk or microfilm/fiche is probably a matter of convenience to the organisation so long as it can be demonstrated that they are a complete record. At present in the UK the VAT authorities are requiring that a minimum of a summary by EDI session by supplier/customer containing all details on a VAT invoice is kept in paper form, irrespective of what other records are kept. The specific requirements of HM Customs and Excise are attached as Appendix III.

Transmission and processing records

In so far as the record of the processing and transmissions are concerned, the requirements are much less precise and I suspect will be governed by the investigative need of the organisation (and authorities) should there be a need to prove an EDI transaction; who did it, when, what was it really etc.

General

There are very few clear guidelines, therefore each organisation should positively decide the following:

- If any EDI transaction(s) to be used by the organisation constitute accounting records and, if so, in what form these should be kept for the required time limits.
- The extent to which records need to be kept to conform to contractual obligations and in what form (on-line, archive magnetic media, optical disk, microfilm/fiche)
- The length of time access and transmission logs (relating to selected transactions only possibly) are required to be kept to support possible investigations and in what form they should be kept

It has been suggested that there could be a third party, possibly the Notorisation or Certification facility, who undertakes to retain EDI records on behalf of organisations. To make use of such facilities, if they are offered, organisations should confirm that certain restrictions are imposed by some countries on the location of records do not apply to them and that there are appropriate procedures to ensure that the third party retains all records in a readable condition and that the records are not altered.

Internal Controls in EDI Systems

Basically the use of EDI substitutes electronic transactions for paper, therefore organisations only require to adjust their internal controls for this change, given that those controls were adequate to begin with.

The majority of the communications software contains procedures to identify where transmissions in or out do not conform to the required technical standards for transmission or message structures. If a transmission is received in a technically acceptable form then it is acknowledged as received (Caveat: this does not necessarily mean that it is accepted for action by the recipient). Organisations should implement procedures to ensure that incoming transactions are not lost and are demonstrably processed correctly by the application systems. Organisations using EDI wish to avoid entering into unacceptable commercial commitments through error and therefore need to confirm:

- That adequate tests are included in application programs to inhibit the issuance of erroneous orders, invoices, etc and to highlight for management decision any incoming transactions that are unacceptable (eg buyer over credit limit)
- That the clerical procedures have been amended to take account of less staff and the automated procedures
- The procedures for identifying and resolving errors, including customer complaints are satisfactory

Types of Audit in an EDI Environment

Essentially there are two types of audit that are likely to be performed:

- the financial audit of the organisations involved as suppliers or users;
  and
- a security audit

In addition there may be requirement for:

- a technical audit of some or all of the software/hardware, particularly if these elements are required to conform to specific standards or specifications or are "trusted" elements within the whole of the system;
- a performance audit against contract terms, particularly in the area of service levels and response times.

I will not cover the technical or performance audit further in this paper.

In addition there may also be audits conducted by the fiscal authorities.

The financial audit

Users of VADS

There appears to be little change necessary to the external financial audit of the users of EDI systems except perhaps the extended use of automated audit tools to compensate for the loss of paper audit evidence. Within the scope of the audit the procedures at users to ensure completeness and accuracy of transactions at the boundary of the organisation will be automated and therefore the consideration of these will substitute for the consideration of the current manual, or semi automated, procedures.

VADS suppliers

These entities will require an external financial audit. The audit of their expenses and the usual accounting ledgers would be very similar to the audit of a computer bureau at present. The audit of their income will be different in that it will be necessary to satisfy the auditors that the VADS supplier had accounted completely and accurately for the revenue arising from the message traffic and storage charges in accordance with the contract terms. This will not be dissimilar from the audit of a time share service at present.

Consideration will also be required by the auditors of any contingent (or actual) liabilities arising through failure to comply with the contract terms or through the inevitable technical breakdowns and delays.

Security audits

General

The security of a VADS is dependent on the security both at the users and the suppliers. Security lapses anywhere in the whole system potentially compromise the security of the whole. It is therefore probable that there will be a requirement for external security audits of VADS suppliers either requested by the users or imposed by Goverments. The security provisions and procedures in users and in suppliers will, as well, often be subjected to internal (and possibly external) audit review.

The external security audit would usually result in a public opinion as to the quality of the procedures operated by the auditee within the requirements of the service contracts. I would expect to opinion to be in the form "X has complied with the security procedures laid down in the contract and/or published standards during a specified period". This opinion may be limited by the exclusion from the scope of the work those procedures performed by other parties not subject to this audit (eg the confidentiality of access procedures by users when conducting the audit of a VADS supplier).

The areas to which attention will be paid in a security audit conducted at a VADS supplier or a user are:

Organisation and general controls
Development and maintenance of software/hardware
Contingency planning
Access and confidentiality
Messages and storage

More detailed areas are described in Appendix III.

Conclusion

All EDI systems are based on a series of contracts between the service•users, the service suppliers and third parties who provide services to either the users or the suppliers or both. Any audit work in an EDI environment must be conducted with regard to these contracts as they set out the terms of the service(s) in use.

The need to retain records of EDI transactions and their associated transmission details must be decided by organisations in the light of their commercial needs, the legal and quasi-legal requirements and the perceived need to have information available in case of challenge. The form that the records are kept in also needs to be decided.

There is not expected to be material changes required to the financial audit procedures at either a VADS user or supplier organisation resulting from EDI except to adjust the audit procedures to take account of the lack of paper audit evidence.

There is a need to conduct security audits within the VADS suppliers and users. The scope of a security audit is all the procedures and controls, including traffic reconciliations, necessary to maintain effective security over the system as a whole.

VADS suppliers are regulated in many countries and users of their services are likely to need comfort as to their propriety. I therefore believe that a formal security audit of VADS suppliers will become a requirement in the future.

The introduction of EDI on a wide scale will provide a new challenge to auditors and an opportunity to them to provide new services to the business community as a whole.

The views expressed in this paper are my own and do not necessarily represent those of any professional body. No responsibility can be accepted for any loss, injury or harm suffered by any person or organisation as a result of action or inaction based on this synopsis.

Appendix I

The Contracts

The service contracts extant in the EDI environment will cover, inter alia, the following:

Between the users and providers:

The nature of the service;
The obligations of the parties;
The rights of the parties;
Service levels;
The required security levels in the system;
The charges for the service;
The country in whose jurisdiction disputes will be heard.

In addition these contracts should also specify the access permitted to the parties auditors to data in the system.

Between the providers and the hardware/software suppliers;

The specifications of the required products;
The rights and obligations of the parties;
The ownership and copyright position on products;
The charges.

Between the hardware/software suppliers and the users:

The service to be provided including maintenance;
The rights and obligations of the parties;
The costs of the service.

In addition users and suppliers will have appropriate contracts with their PTT.

Appendix II

Record Keeping Requirements

The following is a brief summary of legal and quasi-legal record keeping requirements.

Legal requirements

The legal requirements vary depending on the type of organisation. The majority of business enterprises are governed by the Companies Acts 1985 and 1989 and the attendant orders in council. Other UK legislation which contains direction on record keeping or disclosure requirements includes:

Local Authorities Act
Industrial and Provident Societies Acts
Friendly Societies Act
Charities Acts
Financial Services Act
Various Finance Acts
Data Protection Act
Employment Acts
Limitations Act

In general the specific record keeping requirements are similar to those set out in the UK Companies Act 1985 Sections 221 to 223, which state in summary:

> The records shall be sufficient for directors to ensure that legal accounts comply with the Act;
>
> A record of all assets, liabilities and monetary transactions is to be kept;
>
> Records of all sales and purchases of goods are to be kept, together with stocktaking details;
>
> Records are to be kept for a minimum of 3 or 6 years depending on the type of company;
>
> Various penalties for non compliance.

Quasi-legal requirements

The quasi-legal requirements arise from many sources; these include:

The Accountancy Profession
Securities and Investment Board and associated SROs and RPBs
The Bank of England
The International Stock Exchange
Trade associations
Government departments
The Inland Revenue
Customs and Excise (VAT)
Supra-national bodies

Rules governing the admissibility of evidence to courts are set out in the Criminal and Civil Evidence Acts. The possibility of being required to go to court exists and therefore systems should be designed to enable any required evidence to be available without undue difficulty.

Appendix III

Areas to Include in a Security Audit

A VADS supplier

A security audit at a VADS supplier would examine procedures in place in the following areas:

Organisation and general procedures

- Organisation structure including segregation of duties.
- The appropriateness of all policies and procedures within the organisation to address identified risks to the service, probably based upon a risk analysis. The regular review of the policies and procedures in the light of changing circumstances.
- Existence of a security policy and security consciousness in personnel employed.
- Personnel - hiring and firing policies.
- Acquisition policies for hardware, software and other supplies including contract terms.
- Review of the terms and conditions (including security) in the contracts with third party suppliers to the service.
- Confidentiality of algorithms involved in authentication and/or encryption within the service.
- Physical security of the sites used in the service.
- Monitoring of complaints from users.
- Review of the security procedures expected to be performed by users as recorded in the user manual and any procedures exercised by the VADS supplier to monitor performance of these user procedures (if any).

Development and maintenance

- Setting and maintenance of standards for external suppliers to users of hardware and software.
- Setting and maintenance of connectivity standards.
- Development and maintenance procedures for inhouse development inclusive of testing procedures.
- Setting and maintaining the message formats permitted to groups of users in so far as this falls to the supplier. These I would expect to follow EDIFACT or national standards broadly and be agreed by the users or international bodies such as CEFIC, ODETTE, DISH ANA etc.
- Issuance and maintenance of standard software to users of the service either physically or through downloading.

Contingency planning

- A contingency plan exists.
- Alternate Network arrangements exist.
- Alternate Hardware is available.
- Back up copies of up to date software and data are available.
- Back up documentation, supplies etc are available.
- Complete and full recovery can be evidenced to have taken place on completion of the recovery procedures.
- A test of the plan is conducted regularly.

Access and confidentiality

- Development and maintenance of Access procedures and security software for users, own staff and third party staff who are permitted access.

- Key management relating to any encryption algorithms.
- Monitoring procedures for apparent access violations through logons to the system and "odd" system usage.
- Action taken when apparent failure of user to user authentication happens.
- Confidentiality of user profiles on the system.
- Confidentiality of user information on the system.

Messages and storage

- Reconciliation of messages received and sent by users or other networks (to agree to charges raised once traffic evaluated).
- Monitoring of storage utilisation (including storage charges to users) and procedures for ensuring the stored user data is not lost or corrupted.
- Compliance with transborder data flow and data privacy legislation and conventions of the service.
- Maintenance of appropriate history records to comply with legal/regulator requirements and/or to supply copies/evidence to users.

VADS users

A security audit at a VADS user would cover:

Organisation and general procedures

- The changes to general procedures including segretation of duties within the end user departments and DP departments.

Contingency planning

- The amendments to EDP contingency plans consequent on the introduction of EDI.
- The adequacy of the plans to continue business in the event of EDI failure including communication with customers/suppliers, delivery/receipt of goods and settlement of accounts.

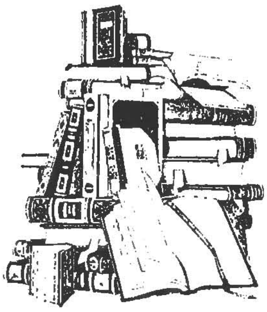
Access and confidentiality

- Procedures to maintain the confidentiality of user login codes, counterparty authentication codes etc.
- Key management relating to any encryption algorithms.
- Monitoring of unauthorised access by computer to either the base applications using EDI messages or the EDI receipt/transmission software/hardware.
- Physical security procedures for transmission devices.

Messages and storage

- Procedures to reconcile messages sent with authorisations.
- Procedures to confirm acknowledgements of messages by the counterparty (if the facility exists in the service).
- Procedures to control incoming messages and ensure they are dealt with.
- Procedures to prevent or detect unauthorised transmission and/or modification of outgoing messages or modification and/or removal of incoming messages.
- Reconciliation of charges from the VADS supplier in respect of traffic and storage.

BOOK REVIEW



TITLE:
BACS Guidance Note – Third Edition

AUTHORS:
CIPFA Audit Panel's IT Group

PUBLISHER:
CIPFA

PRICE:	**PAGES:**
£17.50	34

I liked this little book as soon as I opened it. A brief background to BACS and the volume of items posted each year led naturally onto a section dealing with the user manuals that are available. This in turn passed neatly to BACS users, the processing cycle and file organisation, before dealing with file submission, validation, controls and reporting. Limitations in the controls are dealt with next which lead naturally to recommending some user controls. A final check list brings the whole thing together. It's only a twenty minute read and it does assume that you have access to the actual user manuals, but it is neatly laid out and every sentence tells you something. A worthwhile addition to the audit library.

John Michell

Application Audits on the IBM AS/400

Neil Hare-Brown

Neil Hare-Brown is a freelance Security Consultant. He specialises in IBM Mid-range systems security and disaster recovery.

What shall I do to welcome the new year in I thought? I know, I will write an article explaining the initial steps of auditing applications resident on the IBM AS/400. How could I have overlooked the idea? Anyway, here it is and happy reading.

The AS/400 is my favourite machine with a well structured, some may say complex, and extremely functional operating system. Since the introduction of the AS/400, it has become a very popular machine in the financial services market.

The AS/400 has an architecture which includes a number of services that application developers can build into their applications with a high degree of assurance that the same services will be available on whatever AS/400 the application is likely to run on.

Many of these services will be of interest to the Computer Auditor when they assess the controls built into an application.

How Technical Are You Going to Get?

There are two sides to an in-depth application audit. The first can be seen as being from the user's screen outwards. The controls that the auditor may wish to address here might be procedural, that is, those controls concerned with how well the application serves the business function, and operational, that is, those controls concerned with ther user/application interface, i.e. password control, user heirarchy, user administration, change management etc.

The second part of an application audit can be seen as being from the user's screen inwards. The controls that the auditor may wish to address here will be concerned with the way that the application itself functions. This is the area that I am going to address in this article and, as such, there will be a reasonable amount of technical appreciation needed. Don't lose heart though! If you can, seek and find a competent programmer. (It might be better if the programmer has not been involved in the development of the application that you are auditing.) Show them the article and ask them to explain any terms or concepts with which you are not familiar.

One important point that the auditor should address is whether the application being audited is native to the AS/400 or has been migrated from another platform.

The AS/400 supports applications migrated from the IBM System 36 and System 38. Once migrated, these applications should be amended or rewritten to align with the native environment of the AS/400. For many reasons this is not always done. To avoid complications this article will only address controls associated with native functionality.

The Areas of Control

The areas of control that I will address in this article will impact the security, integrity and availability of data manipulated by an application as well as the efficiency with which the data is handled. These are as follows:

- User Access
- Data Input
- Data Structures

USER ACCESS

The AS/400 provides applications with baseline access control to all objects from which an application is built. This access control cannot be overlooked as it is provided by the operating system of the machine on which all applications depend.

Logical control should be addressed in a technical or system audit of the AS/400 but user authorities on the level which govern user access to a specific application should be evaluated as part of an application audit. The key areas to be investigated are as follows:

- Public Authority to Application Objects
- Group Authority to Application Objects
- Specific User Authority to Application Objects

Public Authority to Application Objects

The public authority to the application objects will control the levels of access that ANY user of the machine has to the application. There is a risk that a lack of control over the public authority might expose the application programs and data to accidental or malicious damage by users that should not be authorised to all or part of the application.

Ideally, applications should not be reliant on public levels of authority to effect the necessary access control to the application services.

Group Authority to Application Objects

Access control through properly administrated group profile authorisation is, in my opinion, the most effective way of allowing users the required levels of access to application objects. The Auditor should first ascertain which groups require access to the application and then confirm this through sample investigation into the actual group authorities to application objects.

Many applications are built around a single or number of user or group profiles. These profiles might be referred to as core profiles. Users are authorised to application objects through membership of core groups or through an access system which adopts the authority of a core profile.

Applications which use this system should be looked at carefully as core profiles are sometimes defined as the global owners of application objects. As owners, the core profiles have (*ALL) authority to those objects and if the method of user authorisation to the application is through core profile group membership or core profile adoption, those users (unless specifically excluded) will also have *ALL authority to the application objects. It could be that those users are only prevented from being able to seriously damage the application through their lack of access to command entry.

Specific User Authority to Application Objects

The Auditor should also investigate specific user authority to application objects. I have not been able to find one good reason why any one user profile, except possibly some IBM-supplied profiles, should be specifically authorised to application objects. If you do come across such cases look into this. Usually the only reasons for specific authorisation are change management oversight, operational reasons (question these), or poor security administration.

A "Library Down" approach should be taken where the Auditor should first ascertain in which libraries the live application objects reside. The authorities to sample objects from each library can then be investigated using the Display Object Authority command (DSPOBJAUT). This command has the facility to send output to an outfile. A great deal of time can be saved if the AS/400 query facility is used to sort and extract records from prepared outfiles. The query reports will show clearly those objects which have incorrect levels of authority.

Software could be written to aid authority investigations. Packages are available which have software which greatly helps in this job.

DATA INPUT

This part of the article addresses the investigation of controls with which every Computer Auditor will be familiar. All applications have a 'front end' where data is inputted and validated. On the AS/400 the way the data is inputted is through special files. Every interface on the AS/400 is formed through the definition of a specific file type. These special files are not like data files (on the AS/400 these are called physical files), although every file type is generated from a source code known as Data Description Specification, more commonly referred to as DDS.

Using DDS you can define physical files, tape files, diskette files etc. The type of file I am going to refer to in this section is the display file. Every screen that an application presents for data input consists of a display file for which DDS is written, (or generated). Display file DDS consists of literals and variables. Fields can be defined in the DDS as being input, output, both or hidden. In addition, validation control can be written into display file DDS so that the display files themselves verify correct data input before the data is passed to the controlling program.

A potential risk exists where the security and integrity of data handled by the application may be compromised through the incorrect definition of display file DDS. There are three ways in which the Auditor can evaluate controls over application display file DDS.

- Test Data Input at Point of Entry
- Review Display File DDS Code
- Review Screen Prints of Screen Design Aid (SDA) or Extended Display
- Review Display File Control Program Source Code

Test Data Input at Point of Entry

This method will be familiar with those who have audited applications before. The testing simply consists of data input through the application screens and verification that fields supposed to be input can be input, those supposed to be output cannot be inputted, and that the cursor is not positioned for input to any hidden fields.

It is advised that any testing of this kind be made with the help of an experienced user and that any transactions recorded be deleted after testing.

Review Display File DDS Code

This is the most time consuming evaluation, but also the most thorough. The Auditor can verify correct field definition as well as any coded DDS validation.

Things to look for might include keywords referring to cursor positioning, non-display, range, input checks, keyboard lock, job log writing and protected fields. DDS functions can be controlled by switches known as Indicators. These can be used to enable or disable keyword function and should be checked.

Review Screen Prints of Screen Design Aid (SDA) or Extended Display

Screen prints from SDA sessions (SDA is used to generate display file DDS), can be used to ascertain field types as well as controls over input validation. Screen prints from extended displays show the field type butes, i.e. fields preceeded with 27H show that the field is non-display. This method is simpler but not as thorough as DDS checking.

Review Display File Control Program Source Code

The source code of the display file control programs can be reviewed to check for correct indicator control and field validation. The Auditor should ensure that all source code printout is the source code directly related to live application objects.

DATA STRUCTURES

There are many ways to store data on the AS/400 and different applications should be designed to access required data in the most appropriate way. Following are some examples of data storage object.

- Physical Files
- Spooled Files
- Source Files
- Message Queues
- Journals
- Logs
- Data Queues
- Data Areas
- Arrays (run time and compile time)

The main object for storing business data is the physical file. DDS can be written for a physical file which will define the record format and field definition for that file.

The AS/400 also provides a special object called a logical file. Each logical file is compiled DDS associated or 'built' over one or more physical files. The logical file defines how and which data is accessed.

In addition to the AS/400 provided access control over physical files which will only provide security for the data at file level, it is possible to provide field level security by restricting users so that they can only access specified data through logical files.

There is a potential risk that this level of security may be required but not provided in the application or that this method of access is used in the application but has not been properly implemented. Either could enable users to access or update sensitive fields to which they should not be authorised.

The Auditor should ascertain from the application development personnel, how data is accessed and whether the methods used are appropriate. Field level security can be assessed by reviewing the logical and physical file DDS and verifying the specific data and object authorities to the physical and logical files.

The physical file can be prevented from being opened by revoking the user's operational authority to it. Access to the required data can then be made by granting operational authority to the logical which defines only those fields that the user is authorised to access, see IBM Security Concepts and Planning manual (Chapter 5).

Well, that's all folks! I hope that the few areas that I have covered in this article have given you a bit of help. If I am threatened heavily enough I will continue to rabbit on about other areas of potential risk that would be of interest to an Applications Auditor in a subsequent issue. Merry Christmas and a Happy Auditing New Year.

Law Specialist Group

The Law Specialist Group has some interesting meetings which you may wish to attend. If you are interested in a particular meeting, just go along to the venue. All meetings at 6 p.m.

Tues 12 Jan 1993	Mr Curtis, Crown Prosecution Service	Computer Misuse Act and Computer Fraud	Lovell White Durrant 21 Holborn Viaduct, London EC1
Tues 9 Feb 1993	Mr Tony Ballard, Partner - Allison & Humphreys	Digital transmission	Allison & Humphreys 40 Artillery Lane, Bishopsgate, London E1
Tues 9 Mar 1993	William List CA MBCS	IT Security - Does it harmonise with paper accounting records?	Mishcon de Reya 21 Southampton Row, London WC1 5HA
Tues 11 May 1993	Richard Morgan	Public sector contracts	Mishcon de Reya 21 Southampton Row, London WC1 5HA
Tues 8 Jun 1993	Mr A Winslade, Hoskyns	Legal aspects of facilities management	Hoskyns Group plc 130 Shaftesbury Avenue, London W1V 7DN

casg
Computer Audit Specialist Group

The British Computer Society

Membership Application

PLEASE RETURN TO
Mr A J Thomas
Treasurer BCS CASG
3 Kings Court
The Maltings
Great Dunmow
Essex CM6 1UX

I wish to APPLY FOR / RENEW (delete as appropriate) my membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 delegates)* * Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal (see over)	£50
INDIVIDUAL MEMBERSHIP (NOT a member of the BCS)	£15
INDIVIDUAL MEMBERSHIP (A MEMBER of the BCS) BCS membership number: ____________________	£10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

PROFESSIONAL CATEGORY: (Please circle)
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Other (please specify)

SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS CASG"
AND RETURN WITH THIS FORM TO THE ADDRESS SHOWN ABOVE

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit   4 = Academic
2 = External Audit   5 = Other (please specify)
3 = Data Processor

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit   4 = Academic
2 = External Audit   5 = Other (please specify)
3 = Data Processor

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit   4 = Academic
2 = External Audit   5 = Other (please specify)
3 = Data Processor

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

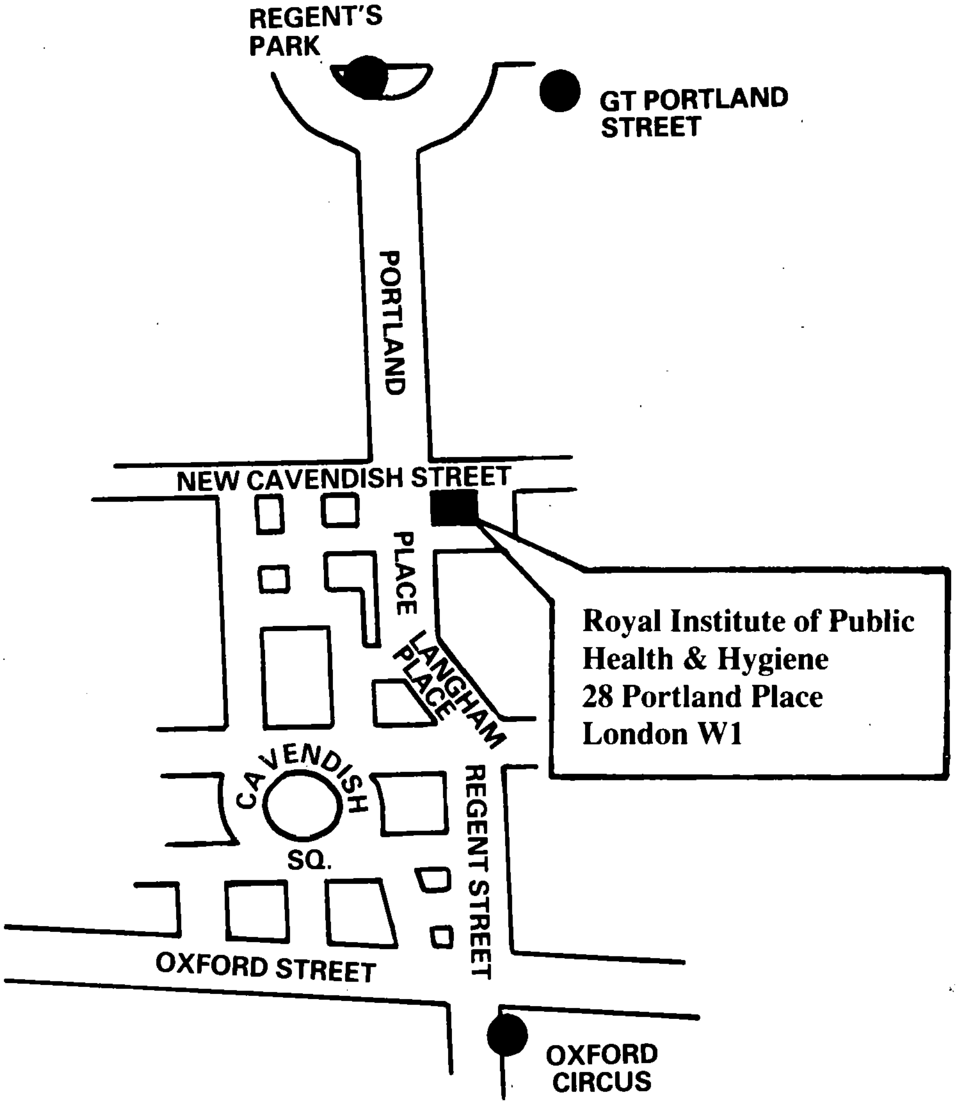
ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit   4 = Academic
2 = External Audit   5 = Other (please specify)
3 = Data Processor

Venue for Members' Meetings



Royal Institute of Public
Health & Hygiene
28 Portland Place
London W1

CASG JOURNAL

SUBMISSION DEADLINES

Spring Edition	14th February
Summer Edition	14th May
Autumn Edition	14th August
Winter Edition	14th November