casg Computer Audit Specialist Group

JOURNAL

AUTUMN 1990

Volume 1, Number 3

The British Computer Society

MEMBERS' MEETINGS FOR 1990/91

5 Dec 1990	4.00pm for 4.30pm	**AUDITING the AS400**	Andrew Henderson *Ernst & Young*	KPMG Training Centre 58-60 Stamford Street London SE1
16 Jan 1991	3.30pm for 4.00pm	**RISK ANALYSIS** **CRAMM** Audit Planning (Joint Meeting with the IIA Home Counties District)	John Bevan *Consultant* John Mitchell *Little Heath Services*	Coopers & Lybrand Deloitte 128 Queen Victoria St London EC4P 4JX
12 Feb 1991	4.00pm for 4.30pm	**Auditing the MVS OS**	Alan Oliphant *Standard Life Assurance*	KPMG Training Centre
12 Mar1991	1.30pm for 2.00pm	**COMPUTER ABUSE** (Half-Day Meeting)	Chris Hurford *Audit Commission* Sandy Douglas *Buxton Douglas Partnership*	KPMG Training Centre
27 Mar 1991	9.00am	Discussion Group **MAINFRAME ACCESS SECURITY PACKAGES**	Greg O'Shea *KPMG Peat Marwick McLintock*	KPMG Training Centre
9 Apr 1991	4.00pm for 4.30pm	**IBM's DB2 RELATIONAL DATABASE**	An IBM speaker	KPMG Training Centre
15 May 1991	9.00am	**ANNUAL CONFERENCE** Building Successful Business Systems		London International Press Centre
		Followed by; ANNUAL GENERAL MEETING		

Meetings are free to members, with the exception of the Discussion Groups, the joint meeting with the IIA and the Annual Conference, for which charges are made.

EDITORIAL

EDITORIAL PANEL

EDITOR

Virginia Bryant

School of Informatics
City University
071 253 4399

DEPUTY EDITOR

Rob Melville

Internal Audit Dept.
City University
071 920 0111

As part of the continuing quest for a high quality CASG journal I am setting up an editorial panel to share the responsibilities for content and production.

I am pleased to announce that one of the first people to offer assistance is Rob Melville who recently joined the City University Business School as Lecturer in Internal Audit. There is a profile of Rob on page 8.

Initially I have approached those people who either expressed an interest via the membership survey questionnaire (18 months ago) or who have written something specifically for this journal. However if you are interested in helping please contact either Rob or me. Some of the envisaged responsibilities to be taken on (probably at least one person per task) are;

- Reporting on Members' Meetings (either by written report or by obtaining an outline of the speakers' presentations in a form suitable for publication)

- Commissioning/Obtaining articles for publication

- Scanning a range of publications on a regular basis and compiling details of items of interest to members e.g.;

  forthcoming courses
  abstracts of articles published elsewhere
  abstracts of presentations/seminar papers
  etc.
  (several people needed for this - info could be put into a database as a resource for both the editorial panel and all members?)

- Obtaining members' profiles and photographs for publication

- Production

- Proof Reading

- Journal Admin

It is envisaged that tasks will be exchanged between panel members, according to personal preferences, at least annually. Four editorial panel meetings per year should be enough to permit a review of previous issues and planning for future ones.

We are also looking for people who would be willing to read and comment on articles submitted on a particular subject or area of knowledge or interest. Again, if you could do this please contact either of us. Your assistance will be of great value to CASG.

In the next issue the column to the left will be filled with the names and responsibilities of others who have agreed to join.

CONTENTS

CHAIRMAN'S CORNER

John Mitchell

Well the new season got off to a resounding whimper, due to a cock-up by the BCS who distributed our annual programme card after the date of our October meeting. I feel that I owe you an explanation, but in order to do so I will first spend a little time in explaining how your Group fits into the scheme of things at the BCS and some of the problems that your Committee faces as a result.

The BCS has some 60 Specialist Groups (SG's) of which we rank about fifth in size of membership and about first in the number of activities that we provide for our members. All told the SG's represent about 25,000 people. The SG's have their own committee, the Specialist Group Management Committee (SGMC), with each Group being represented by its Chairman or other nominated representative. This committee meets every three months and is the main point of contact between the BCS and its SG's. The BCS also employ a person to service the SG's with regard to printing, mailing and other services. This post is designated as the Specialist Group Liaison Executive (SGLE). Now this is where the problem occurred.

Until a couple of years ago, we did our own mailing. It was an onerous task, but we had kept away from the BCS until then for this service, because of the poor level of service received by the other SG's. However, the BCS conducted a lobbying campaign to bring all SG membership lists and mailings in-house and as this coincided with a change in our own Committee membership and the appointment of a new SGLE at the BCS we decided to give the mailing bit a try, but to still maintain our own membership records. Well we had some ups and downs, but once the new SGLE had got the feel for the job there were more ups than downs and we were reasonably happy with the way things were going.

However, all good things must come to an end and the SGLE left for pastures new. Since then it has been disastrous and after the latest debacle of the late mailing some very acrimonious letters have flowed from my word processor to the Chief Executive at the BCS. You may be interested to know that one of the most common complaints expressed at the SGMC is the poor level of service received from the BCS, but this is the first time in my period as Chairman that I have felt sufficiently outraged to put pen to paper. I now know how some of the other SG's must be suffering where they rely on the BCS for both membership records and mailing services.

That aside, is there really anyone out there? We have tried to persuade those people who said that they were interested in setting up branches to take some positive action, but the only response so far has been a deafening silence. Well, this is your chance to tread where no other member has been before. How about it?

Finally, I would like to express my thanks to Brian Kearvell-White who organised our last annual conference and helped to organise our programme for this season. Brian is departing for pastures new and has signified that he will have to leave the Committee. A great loss to us all. Best of luck for the future Brian.

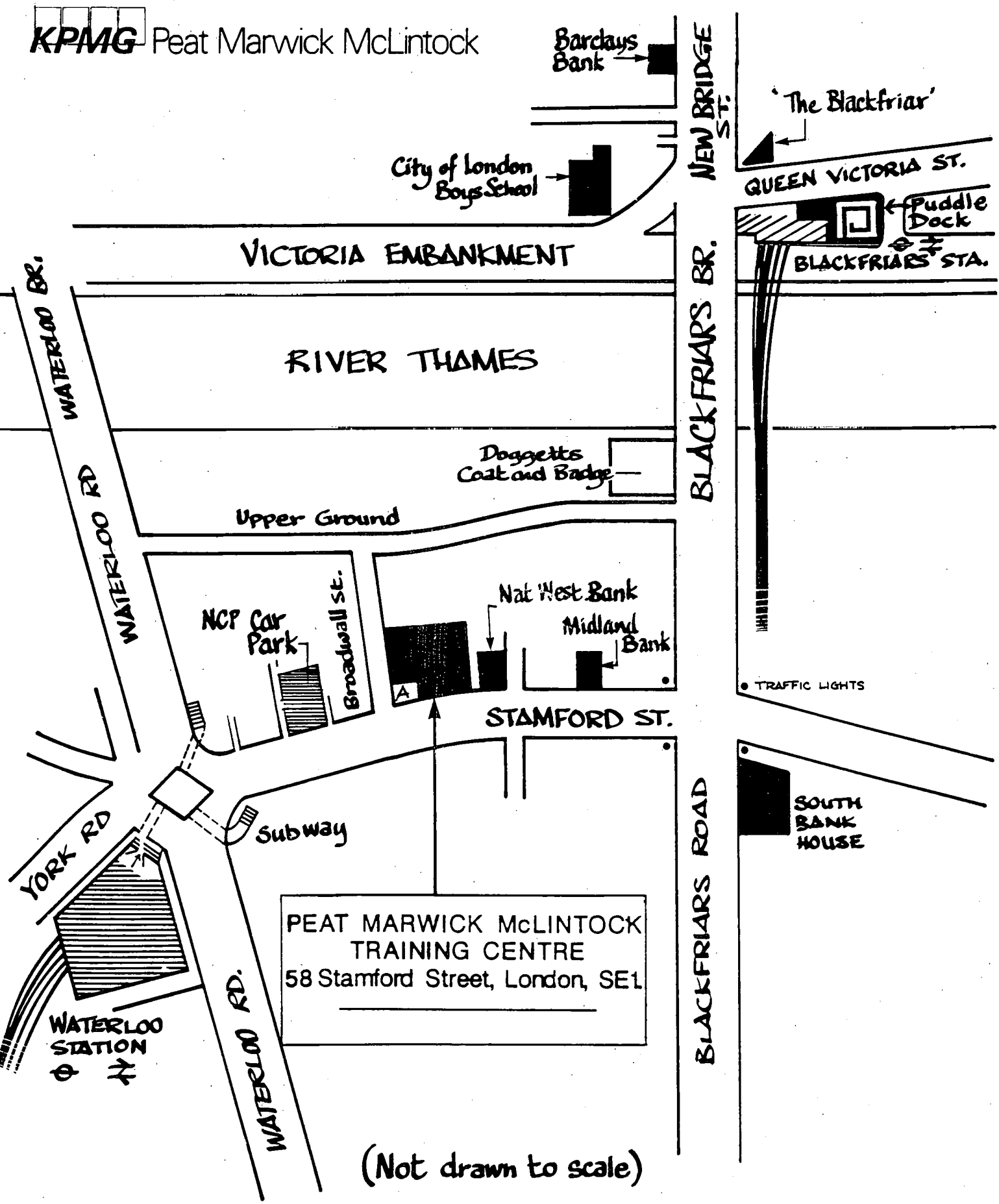
DISCUSSION GROUP SUCCESS

The issues raised during the discussion group meeting on 31st October 1990 suggest that Micro computer environments are not as 'auditor friendly' as they are 'user friendly'!

Over 40 people gathered at the KPMG London Training Centre for an all day meeting of presentations and discussions. Late telephone bookings had to be refused to avoid overcrowding. The internal auditor's responsibility for micro systems, MS DOS as an audit tool and the audit of micro system development were among the topics covered. Many views and practical experiences were expressed during what was generally regarded as a most successful event. Congratulations and thanks are due to Stephen Crowe of Ernst & Young for organising this event.

The next 'Discussion Day' is about Mainframe Access Security Packages on 27th March 1991. Numbers will again be restricted for the March discussion group meeting. Booking forms for this will be circulated with the next issue of this journal.

NEW VENUE FOR MEETINGS



GROUP DEVELOPMENT

Fred Thomas
Treasurer CASG

The Computer Audit Specialist Group is constantly seeking means of improving its service to members, and this was a major factor in the questionnaires which were circulated last year.

Our distribution of membership is such that some members must find that opportunities to attend meetings are few and they cannot hear from people who have gained a practical insight into the sorts of problems which arise in a developing profession. Although we aim to distribute information on talks given in London, this cannot replace the first-hand opportunity to hear and discuss with speakers.

One possibility would be for additional meetings to be held outside London in centres more convenient to groups of members. For this to happen requires local support, knowledge and organisation with the backing of the main Committee. The main Committee is willing to support local development if it can be organised.

A breakdown of the Group's "Country" membership shows that it has 202 members distributed in the following areas:

South East	Bexleyheath. Dartford, Tunbridge Wells, Bromley, Headcorn, Brighton, Worthing & Croydon	16 members
South	Portsmouth, Bournemouth; Swindon, Guildford, Woking, Farnborough, Basingstoke Oxford & Amersham	20 members
South West & Wales	Gloucester, Cheltenham, Bristol, Shepton Mallet, Cardiff, Newport	12 members
West London	Kingston upon Thames, Surbiton, Sutton, Thames Ditton, Hounslow, Brentford & Windlesham	19 members
North & N.W.London	Hemel Hempstead, Harrow, Barnet, Watford & Hertford	24 members
East Anglia	Norwich, Colchester, Basildon, Southend, Saffron Walden, & Cambridge	21 members
Midland	Birmingham, Wolverhampton, Kidderminster, Warwick, Telford, Nottingham, Milton Keynes, Leighton Buzzard, Northampton, Leicester & Chesterfield	27 members
North Midland	Manchester, Wilmslow, Cheshire, Leek & Fylde	14 members
North West	Merseyside, Knutsford, Warrington & Carlisle	19 members
North East	Leeds, Doncaster, York, Newcastle, & North Shields	14 members
Scotland	Edinburgh & Perth	11 members
N.Ireland	Belfast	5 members

Are you willing to help develop the interest in the Computer Audit Specialist Group, increase its local membership, and help provide an improved local service to members in your area? The Chairman will have been in touch with those who offered to help form local branches, but more support is needed. Anyone who can offer to help is asked to write to the Chairman, John Mitchell, at 47 Grangewood, Little Heath, Potters Bar, Herts, EN6 1SL (Tel: 0707 54040).

AUDITING COMPUTER DISASTER TESTS

Malcolm Lindsey
EDP Auditor, Argos Distributors Ltd

If your organisation is dependent on computers - and most are - it will have a disaster plan. A key control for this plan will be regular disaster testing.

This short article suggests an approach to auditor involvement in the testing process. It assumes that there are contingency facilities which include a remote hotstart/warmstart computer site and that nightly backups are stored at a location separate from the normal computer processing facility.

*** Start at the offsite backup storage facility**

The test should simulate the destruction of the main computer facility and all machinery and materials at that facility. Therefore it should start at the offsite backup storage facility. The auditor should ensure that for the recovery no materials are used other than those stored offsite. As they are collected, the auditor should check that these materials include:

- Tape/cartridge media used to back the system up. These should contain all necessary data, application programs and systems software.

- Blank work tapes and computer stationery.

- Recovery instructions. These must include details about which tapes should be used for recovery.

- Computer operating instructions. (Our organisation keeps these on the computer so that the latest instructions are always on the offsite backups.)

- Essential computer manuals, eg messages and codes guides.

- Other reference materials, eg disk and memory directories.

*** At the disaster site**

Travel with the recovery team to the hotstart/warmstart site. Once there confirm that:

- The only materials used are those from offsite storage (or those kept at the hotstart/warmstart site).

- Any telephone calls for assistance are recorded. These can indicate the need for better recovery instructions.

- The recovery team members are different from those attending the previous test This encourages no specific reliance on specialists.

- All difficulties are logged.

- A time log is maintained.

*** User involvement**

Users should be involved in the running and checking of computer processing. For on-line systems, synchronisation of the test with live runs is difficult, but not impossible. The following adjustments may be necessary to the *live* runs:

- Just before backup freeze updating.

- Perform file enquiries on as many files as practical. (Store results to compare during the recovery test.)

- Take normal backup.

- For a short time only allow updates on one terminal and record the sequence of updating so that the same sequence can be repeated during the test.

The above routines have the disadvantage of not reproducing real conditions but have the advantage of testing that the nightly backups stored offsite are complete and accurate - if they are not all the best hotsite facilities in the world could be rendered worthless! They also allow limited testing of the on-line update functions.

Some thought will need to be given to printing the screens used for on-line updating both during the live runs and during the disaster recovery test. This will ensure - that any keying - in errors are taken into account when comparing live and test runs.

*** Other considerations**

- Check that the memory and disk capacities on the disaster machine are adequate. Printer speeds may or may not be important.

- Find out what would happen if a backup tape is broken or unreadable. Sometimes full backups are taken at weekends and incremental backups are taken on weekday nights. If this is so, as long as 2

weeks worth of full and incremental backups are kept offsite the data can still be fully recovered; unless one of last night's tapes is broken.

- If the disaster test involves a national network of leased lines with triangulation and connection to the disaster site, check that the effect of rerouting will not overburden the bandwidths of these leased lines.

- On the day-to-day change management forms there should be a box which is required to be signed in relation to disaster recovery implications. This will ensure that, for changes made between disaster tests, disaster contingency has been fully considered and the offsite copy of the disaster plan has been updated.

- Review how users know which information they have keyed in since the last backup.

*** Audit Reporting**

- Attend post mortem meetings before reporting.

- Report only the crucial issues to management, eg accuracy of results, timeliness of recovery.

- Make a separate, constructive report to the persons responsible for the test suggesting ways of improving contingency plans and future tests.

- Take into account the insurance the organisation has for loss of computers; including consequential loss insurance. The organisation will not want to rely heavily on insurance. It is usually more important to re- establish a service. However, you will need knowledge of these arrangements in order to form a balanced view.

*** Improve auditor's performance**

In conclusion it is necessary to mention the need for the auditor to improve his/her own performance at disaster tests.

- Take adequate notes at the test.

- Enlist the help of computer experts through discussion before, during and after the tests. Encourage their participation in your audit.

- Consider "what if" scenarios with other audit colleagues .

Hopefully the above pointers are useful to auditors starting off in this field. If readers have any comments or additions, I would be delighted to hear from them.

TOPICS FOR MONTHLY MEMBERS' MEETINGS

Your Committee are already planning topics and speakers for the Autumn 91 to Spring 92 meetings. If you have any suggestions about next year's programme or if you know of someone who can give an interesting talk on an aspect of computer auditing please contact John Bevan on (0992) 582439, or any other Committee member, with details.

THE AUDIT COMMISSION'S NEXT COMPUTER FRAUD & ABUSE SURVEY

Chris Hurford
Associate Director, Audit Commission

When the Commission's predecessor body launched the first survey into computer abuse in the UK there was little public interest in the risk of computer misuse but since then, the hacking and virus industries have helped put the subject on many organisations' agendas. Few would have believed, for example, that legislation would have been enacted and the subject of computer crime figure so widely in public discussions.

With a larger proportion of the UK workforce becoming computerate and the increasing advent of desk-top computers, all organisations using IT are, of course, very much more vulnerable to the risks of compute crime. While the speed and accuracy of computers is attractive, the speed of technological innovation may be too fast to allow management and auditors to keep up with potential risks, let alone preventative measures.

The increasing dependence on computing and the race to keep up with developments in technology may well result in management failing to see the need to protect the information it has stored. "Security blindness" is an unfortunate characteristic of many who lose no time installing technology but are less committed to protecting the system from abuse.

While some recognise the costs as well as the benefits of IT, many have experienced great difficulty in identifying reliable official statistics on how widespread the problem is or how much financial loss is actually incurred. But there is no shortage of claims of substantial losses being suffered by the UK business community. £500 million has been cited as the total of annual losses caused by computer fraud though evidence to support such figures is less readily available.

The Audit Commission has sought to provide some help in providing some facts rather than theories on the incidence of computer crime through its triennial surveys which are all available as HMSO publications. Clearly no one can claim to know the true extent of all incidents or be able to put any realistic figure on financial losses and so what does the Commission Survey purport to provide ?

We take the view that in order to install effective measures to minimize the risk of frauds and abuse, organisations need to be clear of the risks they should be protecting against. There is no merit in building a moat if you leave the drawbridge open ! We are anxious, therefore, to record the variety of incidents which have occurred and try and provide an analysis of the systems where controls and safeguards are most lacking. Merely saying that a particular organisation has suffered substantial losses is less useful than knowing how these losses occurred and whether they could actually occur in the reader's own organisation. In fact, this is one of the drawbacks of placing so much emphasis on the financial losses since it can encourage that view that frauds of less than say, £2000 are of little importance rather than to encourage the thought that if the same set of circumstances occurred in one's own organisation the losses could be £20,000 perhaps.

One of the primary purposes of undertaking these surveys, therefore is to contribute to improving controls and minimizing risks. More specifically, the objectives were to identify those aspects of computing which pose the greatest risks; to assess the potential incidence of such risks within the local government sector; and to provide an authoritative survey of UK computer fraud for the benefit of management and auditors generally.

While sophisticated computer systems can lead to sophisticated computer crime, this can make detection costly and difficult. Even so, the past surveys have shown that there is a disturbing lack of those basic, well defined control mechanisms which the text books have been extolling for years. The most obvious control which was absent or deficient in nearly all reported cases of computer fraud and abuse was that of separating the functions of a particular process so that one individual does not have absolute control. The frequency of the incidents reported in the survey suggests that the opportunity for fraud is widespread and that a large number of similar incidents may simply remain undiscovered.

The previous reports have been compiled with the intention of encouraging readers to consider the cases described and assess the impact a similar set of circumstances would have on their own organisations and if it helps focus attention on areas which were thought to be secure but on reflection are suspect, then they would have achieved their primary objectives.

The next Survey at the end of 1990 will continue the overall objectives of our previous research though we will be updating the questionnaire to try and obtain

a more accurate picture of the hacking and virus problems which seem so widespread.

We shall try too to get a better view of the impact of desktop computing and whether organisations have suffered more from micro-based than from other forms of processing.

I should like to emphasize that in compiling the Survey, which is generally regarded as the most authoritative work of its kind, the Commission does guarantee confidentiality. The identities of individuals and organisations are never disclosed and the results are based entirely upon reported incidents rather than second-hand claims.

One of the more difficult tasks in undertaking such a survey is to be certain that the questionnaire lands on the right desk ! We need to be sure that those organisations who have suffered from computer fraud and abuse do get the opportunity to contribute to the Survey but this is quite difficult and depends upon the particular responsibilities for audit and security. Our plan is to distribute questionnaires to a large number of private and public sector organisations throughout the UK in the late autumn of this year and then to analyse the results with a view to publishing the report in the early spring of 1991. If any reader wants to ensure that they do receive a copy of the questionnaire or if they have any thoughts on helping to make that survey more complete then they are encouraged to contact me at the address below.

Chris Hurford
Associate Director
Audit Commission
Nicholson House
Lime Kiln Close
Stoke Gifford
BRISTOL
B512 6SU

PROFILE OF NEW MEMBER OF EDITORIAL TEAM

Rob Melville BA (Hons) MA (London) ALCM MIIA

Rob has recently joined the editorial team of the CASG Journal. He is a Lecturer in Internal Audit at City University Business School (CUBS), where he teaches on Diploma, MSc. and MBA courses and is Director of the Year 1 programme. In addition, Rob teaches computer audit at South Bank Polytechnic and is an active member of the Institute of Internal Auditors; Secretary of the South East District, examiner and author of several articles in **Internal Auditing.**

At CUBS, his main responsibility is for the Diploma/MSc. in Internal Audit and Management; in particular Practices and Computer Auditing. As well as this, he teaches economics and finance, and IT related topics to the MBA IT course. Research interests include audit use of PC operating systems, environmental audits, methodologies and computer literacy for auditors.

Prior to joining CUBS earlier this year, Rob worked mainly as a computer auditor for government, industry and financial services, most recently as Principal Systems Auditor at the Woolwich Building Society.Other experience includes several years in the Services and work on the administration of a radar project.

His principal ambitions are to improve the computeracy of auditors, to develop an intelligent system for systems audit methodology, and to make sure the world recognizes the value of internal review and quality assurance.

EXTERNAL AUDIT EXPOSURES FROM TECHNOLOGICAL CHANGE

Willie List
Computer Audit Partner
KPMG Peat Marwick McLintock

Introduction

Technology is forcing change on everyone in three specific areas:

* It requires a detailed definition of a task, to a level of detail far beyond that expected by a human being - you cannot implement a concept on a computer without all its details.

* The introduction of technology materially changes working methods, over time.

* New business opportunities exist.

In addition many proposed systems involving inter organisational communications, large distributed relational databases, use of personal computers are so complex that it is often difficult for anyone to have a clear grasp on what is going on or to explain it satisfactorily.

There is no current evidence that the quality of application processing will be better than at present despite the improvements in hardware and system software. I fear therefore that everyone will still be faced with the current volume of error in systems. This will clearly make management's and auditors' tasks more difficult.

External auditors will wish to take advantage of the technology to improve the efficiency of their own businesses. The changes will affect the administration systems of external audit firms (eg time recording, debtors, purchase and general ledgers, staff planning, etc) and also affect the methods of delivery of their primary services - audit, taxation and consultancy.

In this talk I shall give my views on the conduct of an external audit in about 1995 where the client is making full use of the new technology making reference where appropriate to the technology being used by the auditors.

The views expressed in this paper are my own.

External Audit

To consider the impact of technology on an external audit we must first determine what it is. Most external audits are governed by statute and address three possible separate objectives:

* To express and attest opinion on the set of accounts under review.

* To report on the quality of internal systems and controls.

* To report on the conformance of procedures and transactions with prescribed rules (usually specific scheme certificates) - which I will not address in this talk

Attest

The basic attest audit objective of stating that a set of published accounts represent a "true and fair" view will be unchanged. In essence this involves the ability to detect material errors in the financial statements be they of omission, commission or presentation. The effects of technological change will vary depending on the different areas of the audit:

* Presentation of accounts

* Appropriateness of valuations of assets and liabilities.

* Accurate recording of day to day transactions

Presentation of Accounts

There will be no material change by 1995 in the presentation of accounts due to technological changes; therefore no effect on external auditors work in this area. Accounts may be prepared using advanced desktop publishing methods by the auditors or clients.

Appropriateness of valuations of assets and liabilities

Technological changes may affect the external auditors in three areas:

* The use of personal computers/advanced query languages to compute provisions etc.

* The valuation of systems/data assets.

* Contingent liabilities/going concern matters relating to the ability to continue trading without the computer systems.

Computations of provisions

The computation of provisions etc is likely to be performed by user written programs, often without documentation (of course the audit staff can read the code/parameters with no trouble!). The auditors will increasingly need to reperform the computations on the basis they believe should have been applied in order to gain comfort as to the results.

The external auditors will still be required to discuss the need for irregular provisions (eg planned plant closures, extraordinary stock losses etc) with the management.

Valuations

With huge sums of money being invested in computer systems and the pressure to value data/systems for security reasons, it is likely that there will be pressure to include these as assets in the balance sheet. As now, with the debate on "brand names" valuation of these intangible assets is likely to prove a thorny problem for external auditors.

Contingent liabilities/Going Concern

Clearly if the client is dependent for its business on the proper functioning of its computers and has not considered contingency planning (or only vaguely done so) then increasingly the external auditors must consider carefully whether an audit qualification is required.

There is also likely to be an increase in contractual disputes between clients and suppliers on the non performance of systems or services of a computer nature. Major matters will concern the external auditors.

Accurate recording of the day to day transactions

There will be a wide variety of book keeping methods employed by clients: some small entities still on manual books and others using the most modern technology. Many clients will still be using the monolithic systems developed in the late 197O's and early 198O's with "user friendly" access tools.

The client's staff are likely to assume that the system will function correctly, particularly if the internal auditors have reviewed it and perform detailed checks on the output.

The external auditors have traditionally gained comfort as to the completeness and accuracy of the day to day transaction recording and the summarization of the transactions to trial balance stage from performing the following:

* understanding of the system and its controls;

* confirmation of the results of processing with external third party sources (eg circularisation of debtors and creditors attendance at physical stock takings etc);

* testing of the proper performance of key controls (eg bank reconciliations, creditor/debtor reconciliations etc);

* limited testing of detailed transactions on a sample basis;

* reperformance of aggregation procedures;

* analytical review of financial and management accounts figures.

Understanding the system

It is clear that the technical complexity of the systems will render a detailed understanding increasingly a less and less effective option for external auditors. It is also probable that many of the controls exercised in the system will be programmed controls which will produce little or no evidence of performance. The extent to which the client's staff will be able to demonstrate the performance of controls will also diminish because documentation of user programs is likely to be poor; staff will assume exception reports are complete without evidence of this; table files of critical data (eg bank interest rates, sales prices etc) are unlikely to be printed out for review, there will remain the likelihood that partial recoveries of distributed databases will provide no evidence of cotimeous recovery, to specify but a few examples. I expect external auditors to increasingly understand the business and obtain a broad understanding of the system.

Confirmations

Auditors will continue to obtain confirmations from third parties. These will provide reasonable audit evidence. The debate as to their worth as evidence will be conducted by those who claim that a confirmation produced by a computer (untouched by human hand) often from information electronically sent to the third party proves nothing. The outcome will be unclear in 1995.

Other tests

I believe that it will become increasingly cost effective for auditors to obtain the full year's transactions from the client and use advanced audit software to perform their other tests. These will be: a scrutiny of the data for anomalous situations; creation of the analytical review information; reperformance of the summarization etc. Clearly they will also require to perform limited tests to determine that the data provided to them is a true representation of the transactions. This will be an extension of the normative audit theories postulated in the early 1970's.

Reports on Systems and Internal Controls

I foresee an increasing understanding at Government Level that computer systems are critical to all enterprises. As a consequence I believe that external auditors will be required by statute to report on the systems in major companies, public databases etc as they are now required to in Local and Central Government and financial institutions. The objective of such reviews is to give comfort that the systems are satisfactory for the future as opposed to the attest audit which largely addresses the past. These reviews will be in addition to the attest audit work.

As now it will not be practical to conduct a full review of all areas at one time unless the entity is small. Therefore these will be done on a cyclical basis.

As now they will concentrate on determining that the management has set sensible policies for systems, effectively monitored the implementation of the policies and acted to correct any matters that would endanger the entity (including perhaps that the entity has specifically conformed to prescribed rules on processing or reporting of certain transactions).

It is clear that with the greater complexity of systems and the increasing use of end user computing these reviews will be expensive to perform, even with assistance from internal audit. I therefore anticipate public discussion as to what needs to be covered and the level of detail of such reviews.

To rely or not to rely

The concept of reliance on systems and controls by external auditors grew out of the practical impossibility to cost effectively check sufficient transactions in large manual systems. Then evidence of performance of controls was clear, there were initials on documents, supervisory staff did initial reconciliations etc. This clarity was lost with the advent of computers and to date the application of the concept to computer systems is unclear despite the efforts of all concerned. In essence the debate could be summarized as "how many less transactions does an auditor check if the computer procedures are first class?". There is no answer!

It is likely that the client's staff will make a working assumption that computer results are right unless demonstrably they are not. Is it reasonable for auditors to do the same and to set up their software to find the demonstrable errors?

What is clear that under the current definition of reliance set by CCAB - that reliance can only be on evidenced controls - there should be no reliance audits by 1995 simply because the paucity of evidence of control will preclude them.

Conclusion

Technological change affects everyone. Principally its effect is to cause changes in working methods. Many current auditing methods which have proved effective for external auditors in the past need revising to determine if they will be as effective in the future or whether other methods are more appropriate.

External auditors will still perform attest and system audits in the future. I believe that the use of the technology by auditors will result in the automation of the majority of their work up to trial balance stage.

External auditors may also develop automated tools to assist in systems reviews in the mid 1990's.

The challenge to external auditors is to harness the technology and revise their methods so as to continue to provide a cost effective service to the community.

MICRO COMPUTERS - MACRO PROBLEMS ?

Neil Morley
System Development Manager
Corporation of London

Background

The growth of micro computing use has been greater even than the pundits imagined. The data processing department's attitudes and performance has contributed a great deal to the demand for 'desk top' computing. The main charges laid against traditional d.p. are:-

The failure to deliver on time, or at all.

The implementation of systems which did not meet the user spec (because the user spec was 'unrealistic'.)

The development of unfriendly applications which users find difficult to use, hard to maintain and from which it is difficult to extract results.

The need to preserve the mystique of computing and the denial that users knew what they wanted.

From this base line we saw the requirement for users to have 'control' of their own machines, to be able to produce reports in the style required 'at the press of a button' and to have screen layouts etc to match their methods of working.

The first sign of progress came with the advent of minicomputers - essentially departmental machines but still hampered by the old failings of the mainframe environment.

Then came the micro computer. Easy to use machines, which could be located on the user's desk, running applications written by businesses who were producing high quality software at competitive prices.

However the old mainframers found it easy to mock. These 'toys' couldn't cope with large quantities of data or large numbers of transactions. They were bound to be unreliable and unsupported. The users would never learn how to program them and worst of all their use would crack the corporate mould and there would be anarchy. The results of this would strike at the very heart of organisations and the centralist power base would be lost for good.

Has this happened? We will examine this anon.

Current stage

The micro computer is now seen everywhere in its various guises- in the home, in the shop, in schools, on the archaeological site, on aeroplanes and in the workplace. We see it networked and standing alone and most importantly as the friendly front end to mainframe services.

The micro has come of age. Some machines can rival the power and capabilities of minis and even mainframes of only a few years ago and yet they are in the hands of the 'non-professionals'. The power-to-the-people revolution has like all struggles given birth to still born children, created enemies, become at times apparently uncontrollable but it has produced very significant benefits.

Problems

There is a veritable catalogue of problems associated with any end-user computing but with the micro computer the difficulties can be very far reaching.

Purchasing

Let's get away from functionality for a moment and look at the economics. The first worry is in the traditional approach to business equipment purchases when items cost in excess of £2k, for example. The perceived wisdom has always been that a retailer should be selected who would offer a substantial discount in return for a high value/volume order spanning 1, 2 or even 3 years. However four factors now militate against this arrangement. Fluctuations in rates of exchange limiting purchasing power, competition between retailers leading to loss leaders and other special offers, the poor life span of many micro computer retailers, and fourthly the rapid change in technology.

Thus we have seen the users circumventing the central purchasing route in favour of short term price advantage. However this benefit can hide poor after sales support, contractual difficulties, invoicing confusion and incompatibilities.

Incompatibilities

We all have met the expression that the only IBM compatible is another IBM. Well to a large extent this is true. Many machines have their own idiosyncrasies be it in their screen handling, numbers of expansion slots, etc. even if they claim to be fully compatible. As for non-compatibles the extent of their non- conformity is boundless. This all leads to user dissatisfaction when one machine cannot read another's discs, when certain software will not run, when modifications are not available, when networking is impossible and when access to the corporate mainframe is not achievable.

Since the traditional position has been that central d.p. will get you out of a fix the users turn to d.p. only to be told that this is the price to pay for d.i.y. So as well as the physical difficulties, cultural differences have arisen which can lead not only to bad feelings but also to the entrenchment of hostile attitudes.

User Satisfaction

We must ask the question whether this new found freedom has given the users greater satisfaction? The answer has to be yes and no. For the committed enthusiast the micro has fulfilled its offer of bespoke systems, ease of use and timely reporting via straightforward tools but the micro has still not solved the problems for the un-educated masses.

There are still some new users who expect systems to be installed with all the data already loaded and what is more the data is assumed to encompass all the new items which have yet to be collected. Some new users even expect someone else to keep their data up to date. With all the encouragement in the world users still discover, the hard way, why regular backups should be taken and why meaningful names should be given to files and documents etc.

As for software there is ample evidence to substantiate the view that many purchases are made on the strength of the advertisement or on the salesman's word. There is generally too little hands-on trialing of software, and the professional, functional testing (including end of year routines etc.) are often ignored. With this situation being a common default what chance is there of the auditing requirements being considered. Similarly the desired examination of security and data- integrity features go by the board.

Now for hardware. The one area where a strategic view is essential is here. So many users are mortified to find that when they require access to networks, mainframes, fax, telex and viewdata services that their machine is not adaptable or that no one makes the necessary 'add-ons'. The truth is very different from those TV ads where the executives stroll in from the car park with their portables to whack out the company profile in less than the time it takes to make a cup of tea. As for those graphics - well who told you need £2.5k of laser printer or a decent colour plotter - and as for printer drivers in your software - what are they? Oh, by the way don't forget you need to have selectable fonts.

Many users have rightly tried to keep up with the trends but they have had poor advice and very poor education and training. The potentials of the micro computer are often missed and user disappointment is often commonplace.

Corporate Data

The need to share data across several user groups is often missed especially if one of those potential groups is audit! The danger of stand-alone micro computers to a corporate body with centralized accounting, is great. If I remember correctly it was Plessey who some years ago realized that they no longer had a grasp of departmental accounts or record keeping and relied upon aggregated totals etc. to balance the books. The audit task became impossible. So the company removed all personal computers and told everyone to use the company machines which were updated to offer services more akin to the micro environment. Things have moved on and now shareability is easier between users in the same group or via the company mainframes and minis. With the adoption of bridges between networks departments can even talk to each other! But even this needs a bit of applied sense and hard work to ensure that suitable security masks are in place, that passwords are changed regularly, that auto-log off is implemented (if possible) and above all that the output from one machine is acceptable to another!

The downloading of data from the mainframe to the micro for further manipulation is now commonplace but how should the extraction process be controlled. Who is allowed to extract, what tools do they have access to, what data bases can they look at, how is their use of mainframe time scheduled and charged. It is even more hair-raising when we look at uploading. All the previous comments apply and in addition two major dangers should be considered. Firstly what software controls are in place at the mainframe end to prevent duff data from corrupting the database and secondly are there guards to prevent the simultaneous uploading of a virus?

Enthusiasm v Professionalism

I have to be careful here because the two terms are not mutually exclusive but without the professional approach to micro computing much of its value and credibility is lost. There really is no excuse to forget to produce a specification of requirements, a design brief, system documentation and a user guide. Nor is there an excuse for the development of applications which have little or no data vetting or validation because too much reliance is put on to the current operators personal knowledge of the procedures involved. Too often we see micro applications wither away when the 'driver' leaves and then the design cycle has largely to be repeated. This re-invention of the wheel also exists on a department to department basis and it is all too common to find groups of users employing their own application which is perhaps 80% or more of the application in use by their colleagues.

The enthusiast can also burn up corporate money by the fanciful justification of 'go faster' bits or specialist utilities which may be required on very few occasions and would be better justified for use by a peripatetic support group.

Staff morale

The evolution of the micro computer has produced a two edged sword in terms of morale for staff and a dilemma for management. The enthusiasts are apparently able to 'get away with murder' in the non-professional approach to the development of applications and in addition they are seemingly little constrained by the corporate strictures which are applied to d.p. department developments. Whilst this situation is often biased, the perception exists which helps fuel an us-and-them feeling which is bound to worsen co-operation and mutual sympathy. The most galling aspect for a mainframer is that the facilities and ease of use which can be demonstrated by the PC user often puts the mainframe services to shame (on the face of it at least).

The dilemma for managers arises in two areas. The first is that of career prospects for the staff who may exhibit two extremes of view at the same time by claiming that they want to be involved with the new and desirable but would not sully their hands on anything which is not housed behind locked doors in an air conditioned sepulchre. The second worry is in terms of the computing hippocratic oath - "thou shalt provide facilities to meet the users requirement (unless....insert here the standard site get-out clause....)". When asked, the users require "instant" response times, full colour screens, 24 hour access, seamless downloads to their pet WP or spreadsheet package and a menu driven system to provide editing and reporting facilities. **And why not?**.....so how can this be done without compromising traditional standards (or should I say just 'traditions'?) There are several well trodden routes to a solution but my task today is to talk about problems. If anyone requires to see me later to discuss solutions my consultancy rate is less than that charged by most accountants.

VIRUS infection

One of the greatest perils of recent times is the infection by virus. Whilst I am sure that you all know of the potential danger it is worth re-iterating. Not only can we find stand-alone PCs which are infected but that infection may reside in the file servers of Local area networks. However the most heart stopping scenario is that of a virus being uploaded to the mainframe. What steps should be taken to prevent this?

Data Protection

The Data Protection Act is well established but the standard set by good d.p. departments for control or development, access control, output distribution and of course registration, is liable to be overlooked by the ill-advised micro developer and the consequences of this lack of proper concern could be very far reaching indeed.

Conclusion

The growth of micro computing has been explosive. The micro computer has become a viable computing tool and has provided a large number of considerable benefits. As with any evolutionary process there are difficulties to be overcome. I suggest that the child has reached adolescence very quickly and we need tp provide a package of parental guidance to modify its potentially destructive tendencies and to channel its energies for the best purposes. Most of all however, we need to tell our neighbours that this youth should present no terrors for them and that it should be taken into the community without reservation or prejudice.

THE IT MANAGER'S VIEW OF AUDIT

Geoffrey Bennett
Prudential Portfolio Managers Limited

This is the text of a talk at the CASG meeting on 6th November 1990

INTRODUCTION

Thank you for giving me an opportunity to explain an IT Manager's view of Audit. Clearly my view is a very individualistic one. Whether it represents the generality of IT managers would be difficult to judge. I suspect it can't - I suspect that in practice IT Manager's reaction to Audit cover the whole spectrum of human emotions - from hostility bordering on the paranoiac to welcoming bordering on the submissive:

Spectrum of Responses

I would like to think my view lies somewhere around the Welcoming.

Not because I am by nature a benign sort of chap; more because I see Audit as a resource I should be using similar to, say, consultancy.

So for me the question of an IT manager's view of Audit is more usefully phrased as how best can the IT and Audit functions work together. I am thinking particularly of internal auditors.

- As an IT Manager my interest in Audit is their scope for adding value to the IT contribution, and thereby to the enterprise.

- my interpretation should provide job interest and satisfaction from the Auditors point of view while staying with in the statutory duties of Audit.

The problem is probably the extent to which Audit's separation of duties can be pushed. I would argue for a close liaison between the 2 functions, with Audit contributing strongly to the design of Systems and operating procedures before they are signed off.

This is probably welcomed by the individual, particularly the more confident and well trained auditor. His or her boss however may be less enthusiastic, as he sees the impartiality of the Audit viewpoint in danger of being compromised by a too close involvement in the design of solutions which the Audit function is required to comment on.

So the central issue for me, as a busy IT manager, is to what extent I can call upon Audit to help me write better systems, operate safer networks etc., without actually high jacking scarce Audit resource and subverting their first duty, an impartial judgement of the work of my department.

THE DP MANAGER'S ATTITUDE

An Objective analysis

So much by way of introduction. Let me return to the title of this talk - the IT Managers view of Audit and the fact that the IT manager's attitude will invariably be a mixture of the rational, objective viewpoint, and a subjective possibly defensive emotion.

These two reactions are in conflict . On the one hand the IT Manager will recognise the need for an independent assessment of his installation and indeed should welcome an impartial evaluation.

Beneath this veneer of rational agreement lurks an emotional fear that something quite nasty will be discovered in the IT woodshed. Close co-operation with the Audit team will only hasten exposure of the IT department's shortcomings and by implication the very manager who is required to co-operate with the Auditor. I am being asked to assist at my own execution.

To diagnose the DP managers attitude to Audit one might start by considering the way an IT Manager spends his time. This will clearly vary depending on the problems the Department is currently facing and the strengths of the IT Manager and his team. Paradoxically the IT Manager will spend more time in those areas where his is strong than where he is weak.

Thus if he is a bit of a whizz on LAN's then he is likely to devote an unreasonable amount of his time and energy comparing the relative merits of different LAN technologies, even as his systems remain undocumented, there is a crying need to recruit staff or whatever.

One way of objectively assessing where a DP managers priorities should lie is to consider his budget. It could be argued that the IT manager should divide his time in proportion to the way in which he spends the company's money.

Such an approach might give the following breakdown.

This kind of breakdown immediately suggests a num-

ber of things:

- (1) Your average IT manager has a wide range of quite different work areas to worry about, and will not be proficient in all of them

- (2) He must therefore delegate control and in particular the construction of secure procedures, to his team, who are likely to be of variable quality except in those areas where the manager has been able to defy the normal laws of staff turnover and to build up over the years a consistent high quality department.

- (3) It follows from this that the IT department will benefit from all the specialist help it can get. The DP Auditor could be of enormous benefit in helping our beleaguered manager.

- both by advising him generally of the areas of expenditure at most risk - and by investigating specific situations which the 2 parties agree need looking at.

The central thesis of my talk is that there is in most installations enormous potential for the DP Auditor to assist the organisation by taking a deliberately constructive view of his role in auditing of the IT department.

This is very much easier said than done. It is inevitable that the nature of running a DP Department is getting more complex.

Time was when the DP activity was concentrated on building systems from some kind of user specification, testing the product and then implementing it.

With experience we learnt to segment these activities into a number of logical steps. Later we coined terms like 'life cycle' and 'methodology' to describe the process.

Dividing the system-build process into a number of discrete steps provided hooks for audit reviews. It was relatively easy to see just where an audit inspection was appropriate.

The scene has moved on from this basic model. There are all sorts of peripheral activities that fall within the DP activity, where I think audit can play an invaluable role.

IT ACTIVITIES

1. Strategic Planning

There is an increasing emphasis on connecting DP development not with the wishes of individual users, but with the business as a whole. Before one would capture the requirements of one user, or at least a limited number of user demands. Auditing the extent to which the system design satisfied those requirements was relatively straight forward. Cost justification involved a relatively few variables, and a cost/benefit equation easily derived.

Strategic planning calls for a quite different approach both by the staff employed on the exercise, and the criteria by which one judges results. The cost/benefit equation is subordinated to more intangible concerns with general business direction and objectives, and the role of IT in meeting those objectives. The audit decision is whether to join the action at this high level, or to suspend judgement until definable activities emerge and can be evaluated.

A subsidiary problem arising out of strategic overviews is the conclusion that systems need replacing, often at huge costs as years of man-effort building the previous generation of systems faces a write-off. We are experiencing the problems of a mature DP industry, going through the process of investment replacement. Those first generation systems built up in the DP boom period of the late '70s and early '80s need replacing.

2. Development Disciplines for Small-scale Work

At quite the other end of the scale is the control of small scale work which has had an enormous boost from the PC revolution, or more accurately, the development tools available from PC and other database environments.

The tasks of encouraging exploitation of these tools, yet somehow controlling the result, is a challenge that faces the DP Manager and the IT Auditor alike.

There is a vicious spiral at work here.

As users build their own local systems, they become less dependent on the mainframe or central systems. Their interest in maintaining reliable data diminishes as they build up their own local alternatives.

The centrally held data loses its exclusive role of report production which hastens its demise as the one repository of accurate data - which in turn encourages yet further local systems.

Again we are looking at a problem of control that faces the IT Manager and his audit colleague alike.

End User Computing is taking us down all sorts of avenues, each of which needs careful monitoring.

3. Management Skills

Associated with the widespread availability of friendly, powerful software I think I have detected another phenomenon - the reluctant manager.

When systems development was a relatively straight forward, hierarchical process, career progression was well understood.

In general one moved up the ranks of programmer, analyst, project leader, team manager.

My very personal theory is that we are increasingly seeing whole areas of work where intellectual and financial rewards equivalent to the traditional project leader can be obtained by staying within the technical spectrum. PC software specialists, communications experts, business analysts can all enjoy a succession of stimulating jobs, well reqarded, without having to concern themselves with the hassle of managing teams.

Developing experienced team leaders prepared to swap the pleasures of technical work for the doubtful privileges of managing their colleagues is as much a challenge today as it was 20 years ago. Indeed I find it more difficult today than ever before.

The absence of good team managers again poses problems of control that must be worrying to the IT Manager and indirectly to the audit review.

4. Outsourcing of Work

At least on the face of it, one way out of the dilemma of managing projects is to outsource the work rather than run large in-house teams.

This is becoming an increasingly popular weapon in the IT Manager's armoury of solutions.

Clearly the control challenge does not go away in this mode, it simply changes shape and becomes more pointed.

The IT Manager and his project managers now face the real world of negotiations, evaluation, selection and the potential for very expensive mistakes.

A whole new set of skills is required, for which the traditional work of the DP manager may have barely prepared him.

He will need all the help of the contracts department, and, I need hardly say, the audit department if he is to exploit the advantages of contracting work outside. In its full form we are talking Facilities Management where it takes an average of 9 months to set up a satisfactory contract between the 2 parties.

So plenty of challenges facing the IT Manager, calling for a high degree of active and constructive co-operation between the 2 departments and an excellent understanding between the senior people involved - a degree of openness and trust which will be lacking unless both parties really work at bridging the gulf.

The key is therefore to establish a rapport that ensures the Audit team are welcomed into the IT department as an extra resource rather than a spy in the camp.

One audit friend of mine reckons his profession is seen as the guys whose job it is to bayonet the wounded. Amusing as this description is, it sets precisely the wrong tone.

A subjective analysis

The task of effectively auditing a DP department is therefore as much to do with establishing mutual respect as it is with sound audit technique.

So what about our IT Manager's subjective view as opposed to the objectives analysis of his workload?

As I have already indicated, no matter how rational and correct it is to have an independent view, deep down the IT Manager will be nervous, if not down-right fearful, that something really quite nasty will be said about him.

When you think of it, the arrival of the auditors is probably the only time the DP Managers is faced with having to account for himself in a technical sense. In many organisations (if not most) IT, for all the emphasis on end-user computing, the proliferation of PC's and electronic office services, is still seen as a black art.

The IT manager's boss is often not computer literate, the users either cowed into submission, or hell bent on doing their own thing.

Even today the IT Manager works unchallenged - no one in the organisation has much of a view on say the optimum number of Systems staff, much less the choice of a programming language or the need for more discs. This contrasts with say the marketing, personnel, finance or supply departments, where the tools of their respective trades are relatively easy to understand and discussed with some ease and comfort

by the Board and users of those services.

The IT Manager on the other hand may well go unchallenged for most of his time; the arrival of the audit team represents a rude shock to his sheltered world.

Thus the IT Manager is likely to be even more sensitive to this intrusion on his closed world, than his colleagues in other functions.

THE AUDIT RESPONSE

If all this sounds negative, my apologies, it certainly is not intended to be. It simply sets the scene for considering the circumstances most likely to provide an effective working relationship between IT and Audit. I think the analysis I have suggested represents real opportunities, both of approach and of content.

Approach

The Audit manager clearly needs to be very good at marketing his service. External auditors of course know all about this. For internal auditors the need may not always so clearly seen. There are all sorts of techniques for raising a department's ability to market itself to its fellow departments. These techniques are based on those developed by organisations marketing their products to the outside world, but which can be applied to the internal scene.

Essentially good internal marketing is based on understanding your client department's objectives and of orienting your product to fit those objectives - ie producing what your customer wants rather than what you happen to be good at making. It is also crucially important to make visible both what you can do and, when you've done it, the result. So clearly an audit plan is required, but one very carefully tailored to the target department, meeting the concerns of 3 parties: audit; the IT Manager; the Users.

Content

I would like to stress the importance of product visibility. My attitude to Audit's potential for contributing to my department rises as I get an appreciation of just what the Audit function can do for me. Too often one's initial meeting is a sort of fencing game or a visit to the Dentist. The Audit manager probes a defensive IT department for where it hurts most and in response the DP department closes its mouth tight. If in so doing it traps the Audit Manager's fingers, so much the better!

I think it helps if the Audit department can come along with an audit plan and take time to explain how they go about their audit, what kinds of things they typically look at, how they might help the DP department in specific areas. Immediately the IT manager relaxes - he's looking at a methodology, possibly a schedule, things he recognises and can work with.

The Audit manager can then begin to draw out those areas where he might apply the techniques, thereby possibly supplementing the IT department's resources. The Audit Department will of course have its own, agenda. It will want to look at specific application areas, but to lead off with that suggests a determination to expose some area of weakness rather than work constructively together.

This initial framework strikes me as of great importance. Handled right it can lead on to the Audit department receiving support for all it wants to do, at the same time giving the DP department rather more than just a list of shortcomings.

Besides a visible action plan what else am I, as a typical IT Manager looking for? Possibly three characteristics:

Experience/second opinion/judgement

They sound rather similar, but are subtly different.

1. Access to experience

Audit have one crucial strength as they enter the IT Manager's domain. They have wide experience of the entire organisation. Their work takes them into all the nooks and crannies of the company. They are consequently able to provide our IT Manager with insights he and his staff would otherwise be lucky to come by.

I think Audit should play unashamedly on this major strength - their comprehensive knowledge of the organisation and what it thinks of IT.

2. Second Opinion

Frequently the IT Manager occupies a lonely position - I referred earlier to the gap between the IT Manager and the organisation's understanding of what he is trying to do. The normal feedback channels between the IT Manager and his users don't always operate as effectively as they might. In these circumstances Audit can provide that second opinion on the IT department's plan that may otherwise simply not be available.

3. Judgement

A second opinion is most valuable on the highly judgemental issues, and a counterbalancing view necessary. For example the classic dichotomy between good access to information and security. IT Managers are, in the main, paid to assemble and make available, information. But accessible information conflicts with security of access. This battle ranges at all levels - the conceptal ("who in the company should see what") to the very detailed ("how best do we construct passwords"). The IT manager will get a view from his user, who may be wildly promiscuous with his data, or, more likely, paranoically secretive. Arguably a more useful judgement on the availability of information would come from the Audit manager.

SUMMARY

I have perhaps laboured the point of joint cooperation. It is because I see this as a key to maintaining an excellent relationship between the IT and Audit organisations, which is necessary if the potential from an audit of an IT department is to be realised to its maximum advantage.

I have tried to present the IT Manager's point of view - his need for help which applies regardless of the resources available to him over the years. I have managed both large and small DP departments. In the large arena I have been so distant from the day-to-day controls that I have found the input from an independent audit invaluable in telling me about matters over which I had control but little real knowledge. In small departments, I have found there is too little resource and often too little appreciation of the need for controls, so that the disciplines identified by Audit again are invaluable. As you are no doubt aware there is a growing trend towards distributed, or in my view, fragmented, IT centres. We are seeing what David Butler, of Butler Cox, refers to as a re-run of the "60's" movie, when decentralisation was much in vogue. I think this is dangerous from the point of view of controls in IT. The 1990's version is an extreme hands-off attitude on the part of head office, with bottom-line performance as the only index. The result is a proliferation of small IT units, with out the traditions of security and control built up in the established central sites. As companies decentralise their service departments and focus on bottom line results they dispose of expertise which a large central group can carry, but which a decentralised profit centre can not. Out go the standards officers, database administrators and other guardians of the corporate enterprise. The local DP Manager loses this specialist advice and yet he is in growing need of guidance.

One obvious area of concern is security. There are by my count five separate statutory papers of which the DP Manager must be aware:

Health & Safety at Work Act
Telecommunications Act
Copyright, Designs & Patents Act
Data Protection Act
Computer Misuse Act

There is no way on earth any but the largest organisations will be in a position to monitor the requirements of this mass of legislation and then translate it to operational considerations. The Harvard Business Review recently published an article drawing attention to the "dogma of decentralisation which is rendering countless companies incapable of transferring knowledge and skills from one part of the company to another". A central audit team seems to me to be one mechanism by which knowledge and skills can be transferred from one part of the company to another. I think decentralisation is raising the need for IT departments to work closely with their Audit colleagues. Either way whether the IT organisation is large or small I am convinced that Audit have a great deal to contribute.

In my view the problem of ensuring effective audits and of getting the IT department to adopt Audit's recommendations, is much more to do with attitudes than it is with the technical process. I am quite willing to accept the blame is almost entirely on the IT side who for, who one reason or another, will want to reject the implied censure of an audit report.

That however is the real world and the typical view of the IT department.

Clearly there is much we, on the IT side, can do to ease the relationship and perhaps I could now throw the meeting open for discussion on this and other points.

PEOPLE

John Mitchell PhD, MBA, MIIA, CISA, MBCS, MBIM

John is now into his third year as Chairman of the Group; his previous roles having been those of Membership Secretary and Conference Organiser.

He has been a member of the Group since 1978 and of the BCS since 1984. He joined the Institute of Internal Auditors even earlier, in 1976, and now has its professional MIIA qualification. He is also a member of the EDPAA where he holds its Certified Information Systems Auditor (CISA) certificate.

John has an MBA, with distinction, from Middlesex Business School, where he majored in financial management and control and a PhD from City University, which was awarded for his research into the use of computers for internal audit planning purposes.

He lectures extensively on the subjects of computer audit, audit management and the control aspects of safety-critical systems. He is a regular contributor to COMPACS and a visiting lecturer at City University and the Middlesex Business School.

Having entered the data processing profession as a data control clerk in the late sixties, John worked his way up the ranks to become a Senior Systems Analyst; having worked in the educational, aeronautical and local governments fields along the way. It was as a data processor that he first became interested and involved in Computer Audit. He turned gamekeeper in the late seventies, when he joined Eastern Gas as an Assistant Audit Manager responsible for Computer Audit. After three years he moved to British Gas Headquarters as Computer Audit Manager, where he spent some six years before transferring to British Telecom as Deputy Chief Internal Auditor.

John has now left BT to run his own consultancy, Little Heath Services, which specialises in Internal Audit matters, but with particular emphasis on the security, control and audit of I.T. and the management aspects of Internal Auditing.

When not working John enjoys rambles in the country, good wine and food, photography and playing bad badminton. He is currently attempting to learn ballroom dancing, much to the despair of his wife's feet!

John D Bevan MA Msc. MBCS C.Eng

John has been a member of the specialist group for many years, and for the last three has been on the committee, with special responsibility for arranging the monthly meetings.

As an independent consultant since 1989, he provides training and consultancy services in internal audit and computer security. He has worked in American and British banks, first as a computer auditor, and then as an internal audit manager. Before this he was "on the other side of the fence", in several IT jobs in computer departments and service companies. He has an MSc. in Operational Research, and is a member of the British Computer Society and of the Institute of Internal Auditors (UK).

He has found the special value of the group to be not only as a channel for learning more about computer auditing, but also as a way of meeting others working in the same area, and for exchanging views and experience with them.

COURSES & ABSTRACTS

COURSES

Details of courses in 'Operational Auditing' (i.e. analysis of how well a corporation uses its critical resources. from; Management Centre Europe (ref 1296-17), Telephone (Brussels) 32 2 516.19.11 ext.934. Fax 32 2 513.71.08.

Title	Dates	Location/Contact
Internal Auditing - Level 1	5-7 February 1991	London CAET 071 242 6855
Internal Auditing - Level 2	28-30 November 1990 12-14 March 1991	"
Internal Audit Management and Planning	20 March 1991	"
Value for Money Auditing	28 February 1991	"
Audit of Small Companies	1 March 1991	"
Getting the Most Out of Your Audit	30 November 1990 12 February 1991	"
The Audit of Human Resources	5 December 1990 2 May 1991	"
The Audit of Building Societies	16 May 1991	"
The Audit of Pension Schemes	7 March 1991 (pm)	"
Auditing in an IT Environment - Level 1	24-26 April 1991	"
Auditing in an IT Enviroment - Level 2	30-31 May 1991	"
Networking	4 December 1990 11 March 1991	"
Efficient Personal Computer Operations	4 March 1991	"
Effective User Control of Computer Systems	21-22 March 1991	"

ABSTRACTS

INTERNAL AUDIT

APC Auditing Guideline - Guidance for Internal Auditors
Accountancy - September 1990

SECURITY

A Concern About Crime; *Crime, serious and petty, damages many businesses.A 'crime audit' could the beginning of a solution.*
CARTY P. - **Accountancy** - June 1990

Old Fashioned Theft in a Hi-Tech Environment; *The author argues that computer fraud is not a new crime, just a problem of a new technological environment offering different opportunities for criminal behaviour.*
SPAUL B - **Accountancy**- November 1990

When Does a Headache Become a Disaster?; *Hot sites recovery facilities are the only solution for 100% protection.*
BURTLES J - **Accountancy** - February 1990

Security I - the sound of silence & Security II - the virus factor
Price Waterhouse Information Technology Review 1990/91

ENVIRONMENTAL AUDIT

The Rise of the Environmental Audit; *Is the 'environment audit simply a way of blocking unwanted intrusions into traditional business practice? Or could it be a starting point for securing competitive advantage?*
MAXWELL S. - **Accountancy** - June 1990

RISK MODEL

Risk: A Model Approach; *Provided the auditor is prepared to make a series of subjective judgements, the audit risk model provides a useful means of articulating stages of the audit.*
ADAMS R. -**Accountancy** - May 1989

New Wine in Old Bottles; *At best, the audit risk model is no more than a new way of saying the same old things. At worst, it turns auditing into a commercial activity. So how useful is it?*
PARIS O. - **Accountancy** - April 1990

MATERIALITY

Materiality; A Factor To Consider; *Some rules of thumb when looking at materiality.*
CHARLES I.- **Accountancy** - April 1990

GENERAL

IT and the Auditor: The Next 10 Years; *The authors argue that the emphasis on developing system controls through technological means is negative and reactive. There should be more emphasis on educational/ motivational or social/organisational aspects of security to discourage potential perpetrators.*
BALDWIN T & WILLIAMS B - **Accountancy** - October 1990

Keeping Control with Post Completion Audits; *Their use can lead to more effective decision making.*
SMYTH D - **Accountancy**- August 1990

Auditing - Last Bastion of the Closed Shop;*Austin Mitchell MP claims that self-regulation of the auditing profession amounts to maintenance of vested interests rather than protection for the public.*
MITCHELL A - **Accountancy**- November 1990

GENERAL (Cont.)

Bridging the Expectation Gap; *This is a summary of suggestions for overcoming the differences between what the users of audited accounts expect and what they get.*
SINGLETON-GREEN B - **Accountancy** - October 1990

Audit Fees of the FT-SE 100 Companies
Accountancy - November 1990

MANAGEMENT COMMITTEE

Chairman	**John Mitchell**	**Little Heath Services**	**(0707) 54040**
Secretary	**Ragu Iyer**	**KPMG Peat Marwick McLintock**	**(071) 236 8000**
Treasurer	**Fred Thomas**		**(0371) 875457**
Publications	**John Hession**	**Hertfordshire County Council**	**(0992) 555323**
Members' Meetings	**John Bevan**		**(0992) 582439**
Annual Conference	**Ian Longbon**	**CWB Limited**	**(071) 220 8495**
Discussion Groups	**Stephen Crowe**	**Ernst & Young**	**(071) 928 2000**
Marketing & PR	**Harry Branchdale**	**British Amercan Tobacco**	**(071) 222 1222**
Membership Secretary	**Peter Martin**	**E D & F Man Ltd**	**(071) 626 8788**
Editor, Group Journal	**Virginia Bryant**	**City University**	**(071) 253 4399**
Long Term Planning	**Bill Barton**	**The Rank Organisation plc**	**(071) 706 1111**