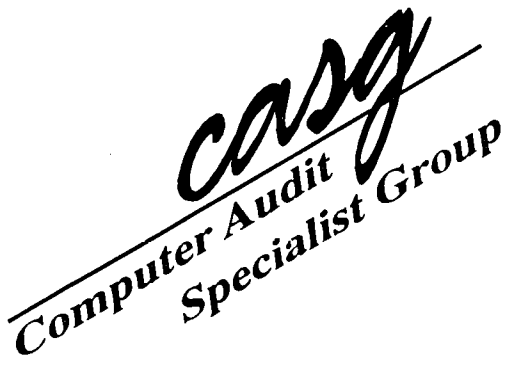
ISSN 0961-9348



The British Computer Society

JOURNAL

SUMMER/AUTUMN 1991

Volume 2, Number 2

MEMBERS' MEETINGS FOR 1991/92

27 Sep 1991	9.00am	**RISK ANALYSIS, CRAMM & VIRUSES (Joint Meeting with with I.I.A. Midlands District Society)**	J. Mitchell *Little Heath Services* J.Bevan *Audit & Computer Security Services* J.Bates *Bates Associates*	Centro, Birmingham
21 Oct 1991	4.00pm for 4.30pm	**AUDITING THE VMS OPERATING SYSTEM**	Alan Oliphant *Standard Life Assurance*	Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
30 Oct 1991	9.00am (full day)	**Discussion Group AUDIT AUTOMATION**		Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
12 Nov 1991	4.00pm for 4.30pm	**COMPUTER ASSISTED AUDITING**	Alison Webb	Royal Institute of Health and Hygiene 28 Portland Place, London W1
10 Dec 1991	4.00pm for 4.30pm	**UNIX SECURITY**	Greg O'Shea *KPMG Peat Marwick McLintock*	Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
15 Jan 1992	3.30pm for 4.00pm	**CONTROLLING SYSTEMS DEVELOPMENT USING STRUCTURED METHODOLOGIES (Joint Meeting with I.I.A.) Home Counties District Society)**		Coopers Lybrand Deloitte 128 Victoria Street London, EC4P 4JX
11 Feb 1992	3.30pm for 4.00pm	**IBM AS400 SECURITY**	A.Henderson *Ernst & Young*	Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
25 Feb 1992	9.00am (full day)	**Discussion Group LEGAL ASPECTS OF THE VARIOUS STATUTES OF INTEREST TO COMPUTER AUDITORS**		Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
10 Mar 1992	1.30pm for 2.00pm	**FACILITIES MANAGEMENT**	D.King D.Earle A.White	Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
14 Apr 1992	4.00pm for 4.30pm	**COMPUTER AUDIT IN INSURANCE**	Christine Osman *National Provident Institution*	Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
14 May 1992	9.00am 4.30pm	**ANNUAL CONFERENCE Disaster Recovery** **Annual General Meeting (Admission free to members)**		International London Press Centre, London

Meetings are free to members, with the exception of the Discussion Groups, the joint meetings with the I.I.A. District Societies, and the Annual Conference. More details will be given elsewhere concerning the Discussion Groups, the Annual Conference and the January Joint Meeting, for which charges will be made.

EDITORIAL

In editorial and academic terms, the summer marks our year end; a good excuse for some self-congratulation and a little 'stock-taking'. The product of the Group continues to develop: we have had very interesting meetings, a successful conference and a lot of enthusiasm for the future. This Journal is gaining its own momentum, with some highly entrepreneurial coups in the advertising department supporting the steady growth in the quality of articles.

In this issue, we have an excellent 'cookbook' for auditing AS400 systems written by Malcolm Lindsey. Papers of this technical quality and audit readability are what set us apart from other journals, and provide sound reasons why computer auditors should align themselves with the Group. The layered approach which Malcolm suggests can also be applied to the writing style which we should encourage: begin with a concept, then work through to low level detail. If any incipient author wishes to rise to this challenge, please contact the editorial team to discuss how they can contribute. Meanwhile, please consider articles on the following;

* Database Management Systems: How Can Auditors Use Them To Their Advantage ?

* Expert Systems: How Should Auditors Approach Them ?

* Experiences Of Auditing 'Off The Shelf' Packages: For Example; Unipay, GL3 and HOGAN

* Involvement With SSADM (or other methodologies)

Ragnall Craighead's article on 'End User Computing' in the Spring edition raised a very important matter (and, at first, one or two of my hackles...). He concluded his piece by supporting 'less of a system audit emphasis' and suggesting 'more concentration on balance sheet and transactions', saying we ought to realise that control features are installed not for auditors' benefit, but as a natural response to processing problems. Finally, he identified a risk that auditors impose anachronistic practices upon modern technology. It took several readings of this paper before I finally admitted that his criticism was probably justified. Auditors, almost without exception, are proud to work for the benefit of organisations. The nature of systems auditing should mean less emphasis on transaction processing (and corresponding strengthening of the systems themselves.) But have we really got our point across ? I am convinced that there is no reason for a return to 'tick and bash, stock and cash' audit techniques; unfortunately, I am now not so sure that we have pleaded our case sufficiently. Practitioners in computer audit must be certain that our customers understand our motives, and the contribution we can make to their systems. We have probably won the battle within the work of our operational and accounting colleagues, but we still have a long way to go in computing, it would appear. So let us make 1991-1992 the year when we all endeavour to raise the profile of computer auditing: write the articles and letters, make presentations, share your expertise.

ROB MELVILLE

CHAIRMAN'S CORNER

JOHN MITCHELL

Well, both the conference and the AGM have come and gone and we are now at that pause in our activities when we gather our strength ready for next season's round of activities. Your committee has organised a good programme for next season, starting with an away meeting with our IIA colleagues in Birmingham in September and concluding with a conference on disaster recovery in May of next year.

During May the BCS was asked to run a conference in Malta on the subject of computer misuse and at the same time to set up a branch of the BCS on the island. Tim Hackwoth, the Director of Services of the BCS and myself did a two day stint on the subject before over 100 interested delegates; including some from the Libyan Department of Audit and Censorship (now that's real audit power!). On the first day we dealt with some of the problems presented by open systems, hacking, viruses and fraud, while on day two we proposed some solutions, including of course computer audit. It seems that computer viruses are endemic in Malta, due to the amount of software piracy that is permitted by the very weak Maltese copyright legislation. However, as Malta is in the process of joining the EEC they are valiantly trying to get their act together; hence the request for help from the BCS and our group.

In the spring I moaned about Windows 3.0. Since then I have purchased Desqview, a similar product, but what a difference. It actually works. As I write this I am using Wordstar in one window, Supercalc 5 in another and dBase IV in a third. I am also running a massive DOS copy of a complete disk directory in background. Installation was easy and took about 3 minutes and the QEMM memory manager is allowing me to run the Wordstar spellcheck, thesaurus and page view sub-programs, which Microsoft's HIMEM manager never quite seemed to sort out. In fact all my old DOS programs seem to run fine and you can even run Windows underneath Desqview and so get the best of all worlds.

Finally, a word on service. A few weeks ago I upgraded to XTREE GOLD, but was unable to install it on my Tandon Pac 386sx machine. This machine has exchangeable hard drives and I have had the occasional problem in getting software to recognise their existence. This was the situation when trying to install the new version of XTREE so I sent a letter to the States asking for help from the software producers. I received a telephone call from them one evening, about 5 days after I had posted the letter, suggesting how I could get round the problem and it worked! Now that's what I call service and Digital Research could learn something from the Xtree people when dealing with queries about DR DOS 5.0, but more about that in the next issue.

I look forward to seeing many of you next season, don't forget to renew your membership; the necessary form has been sent out recently.

NEW VENUE FOR MEMBERS' MEETINGS

Most Members' Meetings for the 91/92 season will be held at a new venue.

This is;

Royal Institute of Public Health and Hygiene
28, Portland Place
London W1

(See map on back cover)

CHAIRMAN'S ANNUAL REPORT - 1990/91

Introduction

Three years ago, when I first had the honour of being elected to this post, I had a number of objectives. These were to:

* amend the name and constitution of the Group to more accurately reflect its activities;
* produce a quarterly journal;
* vary our meeting format to include full day discussion groups and an annual half-day event;
* arrange at least one meeting away from the London area each year;
* increase our base membership.

The first objective was achieved last year when we adopted our new name and constitution (a copy of which you will find elswhere in the journal) and it now gives me a great deal of pleasure to report substantial progress in the remaining areas.

Quarterly Journal

Under Ginny Bryant's splendid direction, our main communication arm with our membership has progressed from a modest photocopied few pages produced in December 1989 to a professionally bound quarterly magazine. The journal now has a proper editorial board, an established format and issue deadlines (April, July, October and January)

Contributions from our members have provided the main material and I hope that more members will consider sharing their ideas and experiences in this way.

Meeting Format

Although our late afternoon meetings still provide the mainstay of our programme, this season we experimented with a half-day format which we believed would be more attractive to our members based outside London. This appears to be the case and we will now be introducing this format as a regular feature in our annual programme.

Discussion Groups

Two Discussion Group meetings were held during the year; the first dealing with micro-computing was organised by Stephen Crowe and the second, which dealt with mainframe security, was organised by Chris Birt.

The format is to have four sessions, each of which is addressed by a speaker for about 30 minutes, followed by about an hour's discussion. We limit attendance to a maximum of 40 members, due both to accommodation restrictions and the need to keep the meeting small enough to ensure that discussion actually takes place in a controlled way.

Both meetings were well supported, even though we make a charge to cover the cost of accommodation and refreshments.

Membership

Our membership records are maintained by Peter Martin and his computer tells us that we currently have 390 members, including corporate members. An analysis of the membership shows:

By type of Membership	1991	1990	1989	1988
Corporate (71 Companies)	245	195	140	139
Individual BCS	57	45	33	35
Individual Non BCS	78	61	34	37
	390	301	207	211

By Discipline	1991	1990	1989	1988
External Audit	48	47	41	38
Internal Audit	290	214	130	151
Other	52	40	36	22
	390	301	207	211

We are now setting course on increasing the membership of the group even further (my own personal target is 500) and Bill Barton, who has responsibility for long-term planning, is tackling this by the direct targeting of organisations and also by the production of a booklet detailing the advantages of membership.

Meeting Venue

Having abandoned our old haunt of the Charing Cross Hotel, due to ever rising costs, we were extremely pleased with our new venue at the KPMG Peat Marwick training centre near Waterloo. Unfortunately, KPMG are now moving their training operation to Watford, so next season we going to use The Royal Institute of Public Health and Hygiene at 28 Portland Place, W1.

Member Meetings

The annual meeting programme was ably handled by John Bevan and Brian Kearville-White. During the season we had planned six late afternoon and one full afternoon meeting, but in the event adverse weather in February forced us to cancel one of the late afternoon meetings at very short notice.

The subjects covered for all our meetings, including two conferences and two discussion groups, were as follows:

1990	Subject	No.of Attendees
19th Jun	1990's - A New Decade (Annual Conference)	45
11th Oct	Data Integrity in a Micro Environment	11
31st Oct	Auditing in a Micro Environment (Discussion Group)	48
6th Nov	An IT Manager's View of Internal Audit	22
5th Dec	Auditing the AS400	41
1991		
16th Jan	Risk Analysis Techniques (Joint Meeting with IIA)	130
12th Feb	Auditing the MVS OS - Cancelled	
12th Mar	Computer Abuse (Half Day Meeting)	33
27th Mar	Mainframe Access Security Packages (Discussion Group)	31
9th Apr	IBM's DB2 Relational Database	28
15th May	Building Successful Business Systems (Annual Conference)	55

On average, the attendance at our meetings is up on last year and if you include the discussion groups and the half day meeting we have actually increased our level of service to our members by some 125% when measured in meeting hours. Not a bad achievement by any standard.

Annual Conference

Moving the date of the annual conference forward in the calendar, from June to May, means that we effectively had two conferences in the season.

The first, which was held in June 1990 on the subject of 1990's The New Decade, was organised by Brian Kearville- White. This attracted some 45 delegates.

Our most recent conference, held in May of this year, was organised by Ian Longbon and was on the subject of Building Successful Business Systems. This subject attracted nearly 60 attendees.

Finances

The report from Fred Thomas, our Treasurer, shows that we are financially sound, but this should not be a cause for complacency as the cost of serving our members has been growing steadily. It is likely that as from next year we will ask for a modest increase in membership fees on a bi-annual basis, rather than go for a large increase every five or six years as we have done in the past. At this stage I must add a word of praise for Fred Thomas our astute Treasurer, who is without doubt the best Specialist Group Treasurer in the BCS.

Liaison with the BCS

During the year John Bevan and myself were involved in specifying the Information System Auditor classifications within the BCS's Industry Structure Model (ISM). The purpose of the ISM is to relate the different I.T. disciplines to each other in a formal way, thus enabling organisations to compare unlike disciplines, such as audit and programming, with each other. This can be quite useful when deciding on grading and remuneration, but more importantly it provides a framework whereby people who move between disciplines, such as computer auditors, can be slotted in at the appropriate level, depending on their qualifications and experience. It also provides a baseline for the production of job descriptions and the like. Although the BCS asked for input from other audit bodies, we were the only group able to respond within the allocated timeframe.

The Committee also continued to be represented on the BCS Specialist Group Management Committee where we made representations to implement service level agreements between the specialist groups and BCS central. This arose because of the variable level of service that we and the other specialist groups had received from the BCS over the last few years. The proposals were accepted and work is now undergoing to define and implement SLA's covering a wide range of activities.

External Relations

Our annual joint meeting with the Home Counties District of the Institute of Internal Auditors was once

again a resounding success with some 130 members (from both Groups) attending to hear presentations on the subject of risk analysis techniques.

During the year members of your committee also addressed meetings of the the Midlands IIA and the Chartered Institute of Management Accountants. This formed part of our policy to increase the visibility of the Group.

On a further topic, and as a result of requests by our members for meetings outside the London area, we have reached agreement with the IIA's Midlands branch to hold a joint meeting in Birmingham in September 1991.

We still enjoy good relations with our "sister" organisation, the EDPAA, and we both circularised details of the other's annual conference and programme of meetings.

Publications

Our joint publication with the Data Management and Security specialist groups,**'The Security, Audit and Control of Databases'** was finally published in April of this year.

Management Committee

The Group's management committee comprises four elected positions (chairman, secretary, treasurer and auditor), as required by the rules of the BCS, and a number of non-elected volunteers. The chairman is required to be a BCS member and it is desirable that the other elected officials are also members, although some dispensation is allowed.

There were several changes to the committee membership during the year, due to changes in members' jobs. The list below shows the situation after the AGM. Each member of the committee has a defined responsibility and where possible there is some "shadowing" of roles to cater for the invariable moves that take place where professional people are concerned.

Elected Officers;

Chairman: John Mitchell *(Little Heath Services)*

Secretary: Ragu Iyer *(KPMG Peat Marwick McLintock)*

Treasurer: Fred Thomas *(Independent Consultant)*

Hon. Auditor:John Court *(ICAEW)*

Members & Associated Responsibilities;

Meetings: John Bevan *(Independent Consultant)*
Meetings: Alison White *(Independent Consultant)*

Press & PR: Harry Branchdale *(British American Tobacco)*

Membership: Peter Martin *(E D & F Man Ltd)*

Journal: Virginia Bryant *(City University)*

Journal: Rob Melville *(City University)*

Discussion Group: Chris Birt *(Ernst & Young)*

Conference: Ian Longbon *(CWB Limited)*

Conference: John Pringle *(Department of Energy)*

Planning: Bill Barton *(The Rank Group)*

Publications: John Hession *(Hertfordshire County Council)*

You may be interested to know that Peter Murray, who was our Publications Secretary until last year, is now working in Fiji for the Overseas Development Corporation. This means that we now have three ex-committee members abroad: Graham Collier in Australia, Bob Aston in New Zealand and now Peter in Fiji. This shows that membership of the Committee can lead to much wider things than the occasional meeting at Peat Marwick's offices!

Conclusion

The past year has been a year of great progress which has only been achieved due to the hard work of your Committee. I would like to propose a vote of thanks to them on your behalf, but more especially on my behalf, as without their generous help and support my job would be impossible.

John Mitchell

"WHATS'S A CONTROL, DAD ?"

PHILIP WEIGHTS

Believe it or not, but auditors do have families. In many cases, long suffering families who endure enforced separation on a frequent basis when spouses are sent on assignments to foreign locations. You return and the kid says, "Hi dad where have you been this week, and what did you do?" "Well son, I've been in Geneva, auditing the bank's new on-line trading system and checking the controls". Usually he loses interest at this point and I ask him if he was good at school, did his homework, and helped his mum at home. But no, he isn't going to let me off the hook so easily this week. "What's a control dad?", he says. I answer saying,"Well, it's something that checks that things get done properly. For example, if I ask you to clean your room, and then tell you I'm going to check the room in 1 hour, then that is a control". That's when he loses interest. Anything remotely to do with cleaning his room must be bad news.

The point is, I kept asking myself the same question for the next few days. "What's a control dad?". From a business viewpoint, is it really just something that ensures the work is properly processed? How does this relate to risk? Most books on audit and control tend to talk about internal control systems being there to reduce risks to an acceptable level, at a reasonable cost. So then we can define control in these terms... to ensure the work is properly processed and accounted for (definitions from auditors always mention the accounting system somewhere), on a timely basis, with risks reduced to acceptable levels. Is this then the elusive Holy Grail? Can I now sleep easily? Can I look my son squarely in the eyes and tell him I do know the answer to his question? Afraid not. At least not yet. Because I am not comfortable with this relationship between risk and control. So I turn to chapter 11 of Hugo Cornwall's book "Data Theft" which covers risk assessment. Maybe the answer is here. It tells me that risks can be reduced, assumed or transferred. In other words, the organisation can spend more money on controls (to reduce the risk), do nothing (risk is insignificant so assume it), or buy an insurance policy (and transfer the risk to an insurance company). Well I agree on two out of three, that is self-insure or obtain a policy, but risk reduction via increased spending on controls is causing me problems. You see, I don't believe that risks can be reduced, and this is where my definition problem lies. I know what a control is, and I know it is related to the existence of risks. But do I know what a risk is? If a risk can be transferred to an insurance company via the acquisition of a policy, then is the absence of adequate insurance also a risk? Is the insurance policy itself a control? If risks can be insured, and the absence of a policy is a risk, then can this risk itself be insured? Help I'm getting confused.

Perhaps the answer lies inside an insurance policy. Here is an example of coverage, "... loss resulting directly from the receipt by the Assured in good faith of any counterfeit or altered paper money or coins". This tells me three things. First, that a risk involves a loss (so no loss no claim). Second, the loss is always directly related to the value of a specific named asset (in this case paper money or coin), and finally the loss is the consequence of an event occurring (receipt in good faith of counterfeit or altered). Other unspecified events would not be covered by this policy. For example, the country issuing the paper money pulls them from circulation (as did the USSR recently), thus rendering them worthless to the holder.

Now where did we get. Well, we have progressed from a control being related to a risk, to a control being related to a combination of three things, 1) the possibility of a loss, 2) directly affecting an asset, 3) caused by a specific event. It is initially the linking of control to asset that interests me the most. We know that an asset is something we own, which is of value, and that may decrease in value via loss, damage or destruction if certain controls are not put into place. "So, what's a control dad?" It is something put into place to protect an asset, to ensure that the likelihood of loss is decreased by reducing to an acceptable level the frequency of occurrence of events that might place said asset at risk". The trouble with definitions is that you can never get the wording right, and 100 people with different opinions will pick holes in them. The important thing to recognise is that internal control systems are not vague, unclassifiable, unauditable conglomerations of procedures, preventive measures and the like. They can be subject to analysis. For example, auditors can list the assets owned by the company such as cash, securities, computer equipment, software, telecoms network, etc. Then by order of value and importance to the company, each asset can be listed with the major risks or events that could occur that might give rise to loss, damage or destruction. Then we can look at the internal control system and cross-relate each control to its corresponding asset/risk combination. In computer auditing terms this is a simple database solution with tables containing asset definitions, risk definitions, and control definitions. These are then cross-related via relational tables. The control system analysis will then reveal any inconsistencies in the design of the controls, the need for additional controls, and the areas in which control testing needs to be concentrated.

But I'm still unhappy with the risk definition. And I still feel that risks cannot be reduced, merely assumed or transferred. There is still a missing link. Something that relates closely to the asset/risk combination but plus an added ingredient. So let's focus on the risk definition. Its three components are loss, asset and event. The first two I understand and accept. The final component is the problem. A risk is related to a specific event, or series of events, that causes loss or damage to an asset. How about an example? OK, the organisation's IBM 3090 mainframe is insured against loss or damage caused by fire, flood, theft or vandalism up to the amount of £400,000 with a £10,000 deductible. In this example we see that the insured events are fire, flood, theft or vandalism. To my mind, the insurance policy is the control covering these events. However, the internal control system is designed to reduce to a minimum the events that might cause the insured events to occur. In other words, a fire can be caused by, or the loss aggravated by, many situations. This includes excessive combustible materials in and around the computer room, lack of a no-smoking policy in the computer room, electrical wiring that doesn't comply with standards, inadequate air-conditioning and environmental controls, absence of fire suppression systems etc. A flood can be caused or aggravated by locating the computer in the basement, below sea or river level, having plumbing pipes running in the ceiling above the computer, lack of plastic covers for emergency use, lack of adequate drainage in the event of an inundation, and so on. These situations, which I define as being threats or concerns, are the potential causes of the events covered by risk insurance coming into evidence.

Therefore, it is the threats or concerns to which the assets or resources of the organisation are exposed that we need to control. Put into simple terms, a risk does not occur on its own, it is caused by acts of people and nature. Let's say the company's cash is insured against the risk of loss by theft. The purpose of the policy is to protect the company IF LOSS OCCURS BY THEFT. The internal control system, properly designed, operates at a more detailed level. It responds to a management analysis of HOW THEFT CAN OCCUR, in order to reduce the probability. For example, we might consider that theft can occur via teller appropriation, in which case the company implements two controls, 1) to limit the maximum amount the teller can handle based on experience and seniority, and 2) daily cash audits. Then the analysis of HOW THEFT CAN OCCUR reveals that a possible threat would be caused by lack of control over cash transfers between tellers, or between tellers and the main cash reserve vault. Accordingly other controls are then designed and implemented. This illustrates that the internal control system is, or should be, directly related to those events which define how a risk can occur. Insurance is a control which takes over when all else has failed, and is effective AFTER A DEFINED RISK SITUATION HAS OCCURRED. The internal control system addresses events that occur PRIOR TO THE RISK BEING PRESENT.

Time to summarise, come to a conclusion, and go home. First, let's not confuse risks and control systems. Insurance companies are in the business of risk insurance, not auditors. Internal control systems do not reduce risks, insurance policies do. Controls are designed to protect assets and resources in order to reduce the threats or concerns associated with them. This in turn minimises the probability of a risk situation occurring. Audit analysis of internal control systems needs to be more sophisticated, structured and technology dependent than has been evidenced in the past. There is much to be done. Computer Auditors should not only evaluate internal control systems within EDP applications and operations. They should also design database systems and software to assist financial/operational auditors in evaluating the adequacy of all control systems within the organisation.

"What's a control dad?". Ah, shut up and stop asking stupid questions.

AUDITING THE IBM AS4OO

MALCOLM LINDSEY

EDP Auditor , Argos Distributors Lunited

This article is aimed at the EDP auditor who has no previous experience of auditing the IBM AS4OO .

The various subjects have been subdivided into levels. The idea is that you cover level one on the first pass and then progress to higher levels as more time becomes available and your expertise increases. This type of approach has been called the Pyramid approach, the "Onion" approach or the 80/20 approach. To the many EDP auditors with scarce resource I hereby christen it the "Only approach" !

The prerequisites of an AS4OO audit are the same as those for any technical audit, namely:

* Physical security and physical access will have been audited (including fire protection, battery backup etc) .

* The auditor will have an appreciation of which potential risks are important to the business or organisation.

* The auditor will have a thorough understanding of the organisation and its segregation of duties.

* There will either be a formal statement of what the organisation requires in the manner of security or else the auditor will, by interview of the appropriate senior business and computer managers, have formed an opinion on security requirements .

Manuals and Getting Started

I suggest that you book some time with the AS4OO Security Officer and work through the interrogation parts of the audit with him/her. Not only is this quicker, it is also safer. Unlike RACF (the security package used on IBM's mainframes) , the AS4OO does not have an "auditor" special authority. You would need powerful access to the AS4OO resources to perform some interrogation tasks yourself. Your credibility would not be assisted if you made a mistake.

Get the Security Officer to show you where the following manuals are located:

* Programming: Security Concepts and Planning (SC21-8083)

* Programming: Backup and Recovery Guide (SC21-8079)

LEVEL 1 AUDITING

Keylock Switch on the System Control Panel

There are four positions to which the lock can be set: Secure, Auto, Normal and Manual. IBM recommend that the lock be set to Secure, Auto or Normal. The reasons given are that the manual position allows the use of dedicated service tools - giving access to all resources - and allows the system to be manually turned off whilst still in use.

Access to the key needs to be restricted taking into account the security and operational requirements . Considerations are:

* Dedicated service tools are also password protected. The password is controlled by the Security Officer.

* Use of the manual position allows the loading of a different operating system from tape. This is not password protected.

* The manual position is required for "cold" or manual IPL's. These should occur weekly in order to clean up the spool file and this will usually be done out of normal office hours.

Security

Display important security related system values using the DSPSYSVAL command . These are:

- QSECURITY: Most installations should have this set at "30" to ensure that users must be given authority to use resources.

- QMAXSIGN: Maximum sign on attempts. This should be 3, 4 or 5 .

- QINACTITV : Shows the time in minutes when an inactive terminal is timed out.

- QPWDEXPITV : Shows the maximum number of days that a password is valid. Usually this should be 30.

- QPWDMINLEN: Shows the minimum number of characters required in a password. This should be at least '6' .

- QPWDRQDDIF : Shows if the password must be different from the 32 previous passwords .

- QLMTDEVSSN : Shows if user can have more than one device session occurring at one time. This should not generally be allowed in order to discourage the sharing of passwords.

Use the DSPOBJAUT command to display the object authorities of the critical objects: QSYS, QUSRSYS and QHLPSYS. The last line of the sceen in each case should read *PUBLIC *USE - this means that the only public access is "read".

* You may not be able to display QUSRSYS whilst the system is busy.

* Type DSPAUTUSR OUTPUT (*PRINT). This will list all user profiles. Check that all users are current employees of the organisation. Check that all IBM-supplied user profiles shipped as password 'NO' have not had password changed to 'YES'. These are all profiles beginning with Q except QSECOFR, QSYSOPR, QPGMR, QSRV, QSRVBAS and QUSER.

* Check that the following IBM-supplied profiles have had their passwords changed since the system was installed: QSECOFR, QSYSOPR, QPGMR, QSRV, QSRVBAS and QUSER. You can perform the check by trying to sign on using the profile name as the ID **and** the password. For each of the five cases you should be denied access.

* Check that the Dedicated Service Tool Password has been changed from QSECOFR. This will involve half an hour at an 'out-of-hours' time as you will need to try to access dedicated service tools and this will require keylock switch to be set to manual.

Dial Up Security

If dial up facilities exist on the AS4OO there is usually justification for fitting dial-back protection as this is very cheap (the protocol converter and dial-back hardware for this costs approximately £1600.) If this is not installed you should recommend that it is.

The dial-back device will contain a data base of valid remote telephone numbers. when a caller dials in, the call will be broken and the caller automatically phoned back before processing commences.

Obtain a list of the user ID's, passwords and telephone numbers in the database and establish that they are current and have been authorised.

Change Control

Check that there are procedures for adding and amending objects to production libraries and that programmers cannot, in normal circumstances, update these libraries. At this level this will involve using the DSPOBJAUT command to display the object authorities of the relevant libraries.

If it is necessary, for operational reasons, for programmers to be called in overnight the normal routines will have to be supplemented with:

* An automated method to detect the event (e.g. detection of use of "firecall" password.)

* Checking routines to verify what has taken place. This will probably mean changing the AS4OO system default for job logs so that the job logs are not automatically cleared as these show all comnands used. This, in turn, will mean having a controlled way of clearing job logs.

* Procedures for obtaining retrospective user authorisation (full printed audit trail should go to the user)

* Procedure for re-installing the change using the normal routines.

* Procedure to change the "fire-call" password.

Disaster Recovery

In the author's view, a key part of auditing disaster recovery is to review the disaster recovery test (for an audit methodology see **CASG Journal** Autumn 1990).

If this option is not immediately possible you should at least obtain confidence that the offsite backups are adequate. If complete backups are taken and stored offsite use the DSPTAP command to list the contents of a set that have come back for reuse. Check that these are adequate. If incremental backups are taken this will probably be facilitated by the use of a package. In this case you should expect a listing of the tapes to be produced as a function of the package. It is possible to use these lists (which should be stored offsite) to audit the incremental backups.

LEVEL 2 AUDITING

Six special authorities can be defined in the user profiles. The sensitive functions are:

*ALLOBJ	allows use and deletion of any object
*SECADM	allows use of security functions
*SAVSYS	allows deletion of data portion of object
*JOBCTL	allows IPL, starting and stopping the system and handling job queues and output queues.
*SERVICE	allows user to access sensitive data.

(Only a user with *SECADM and *ALLOBJ special

authority can give another user *SECADM special authority.)

Use your knowledge of the required segregation of duties to analyse all profiles to review who has special authorities. One way is to use DSPUSPRF USRPRF (user-profile-name) on each profile. A less tedious way is to ask the Security Officer to list the special authorities for all users. If this method is used it is worth asking the Security officer to list some of the other fields on the user profiles such as:

* User Class
* Password of None
* Previous Sign on Date
* Limited Capability
* Group Profile
* Group Profile Indicator

These will be useful at later stages.

Security - Group Profiles

Using the profile list produced above generally get to know about groups. This will entail looking at the fields : User, Group Profile and Group Profile Indicator.

Check that all Group Profiles have "Password of None" set to Yes.

Security - Limited Capability

Limited capability "YES" on a user's profile means that users cannot use commands. On a system wide basis the limited capability can be over-ridden for specific commands .

Use the profile list and a list of system wide parameters to review which users can use which commands.

Security of Production Files

Use DSPOBJAUT comnand to display the object authorities of sensitive files such as supplier master files, payroll files, BACS files etc. It is much quicker to get the Security Officer to explain the output as some of the IBM terms are difficult to grasp at first. You can establish your independence at a later stage by checking the accuracy of what you have been told by reference to the manuals .

On the AS4OO, files reside in libraries. For a sensitive file there will be a more definitive object authority on the specific file than on the library. To fully understand the access you will need to look at both the file access and the library access .

Change Control Continued

A change control package is not expensive. However, if an AS4OO installation has not got this you should at least expect some in-house software to be controlling changes (the IBM AS4OO toolkit provides software which assists in the creation of such software). Check that the software:

* Resides in a protected environment.

* Provides integrity between source and object.

* Provides an audit trail of changes.

* Keeps track of version numbers.

* Cannot be circumvented.

Monitoring of the History Log and Journals

* Ensure that an appropriate person within the installation is charged with the responsibility for monitoring the history log on the AS4OO. Specifically messages in the range CPF2201 to CPF2299 are security related.

* Ensure that an appropriate person within the installation is monitoring changes to the security environment as logged in the QAUDJRN journal.

PC Support and Transfer of Files between Machines

The System Directory contains the user ID and qualifier for users allowed to use object distribution (PC support users and users who transfer files between machines). Use WRKDIR to review these entries and establish that the users have the required authority.

CAATS

Probably the easiest tool for CAATS is AS4OO Query. It will take you 15 minutes or so to find out more about this by using on-line education facilities:-

* On the command entry line, key in GO MAIN and enter (if you cannot enter commands, seek advice within the installation.)

* Option 10 of this menu will give you "User Support and Education".

* Option 9 of this menu will give you "On-line Education".

* Option 3 from this menu will give you a list of options.

* The last option (after paging forward) will give you "AS400 Query Overview".

LEVEL 3 AUDITING

Extend your Knowledge of Security

Read chapter 3 (User Profiles) and chapter 4 (Resource Security) of SC21-8083.

Relate chapter 3 back to listing of profiles mentioned under LEVEL 2 Auditing - Security - Special Authorities.

Tuning and Capacity Planning

In an article of this length only "motherhood" audit guidelines, can be offered. Nevertheless these are useful in reminding the auditor that a review of Tuning and Capacity Planning may be relevant in the audit. Guidelines are:

* Ensure that an individual is charged with the responsibility for Tuning and Capacity Planning.

* Check with the individual so identified and the users that there is an agreed written statement on run time requirements, response times required and the future growth in workload.

* Verify that regular management reporting is carried out and that user management reporting is carried out and that user management have copies of these reports. The reports should include past trends, future predictions and recommended action.

LEVEL 4 AUDITING

Security

Read the rest of SC21-8083.

Recovery (other than disaster recovery)

The AS4OO has extensive facilities for increased resilience and fast local recovery. The manual covering these is SC21-8079. Since this is a large manual you may find the following overview useful.

- Journal management enables fast recovery of database files .

- Checksum protects data being lost when a single disk is corrupted. The system automatically reconstructs the data when the systems program is loaded after the device has been repaired. Typically, disk usage can be increased by 15-20% so there is a cost involved. The auditor should also verify that performance trials are run if this option is to be considered.

- Mirroring protects data by duplicating the disk data of one unit on another disk unit. Typically disk usage can be increased by 30-35%

LEVEL 5 AUDITING

Using the AS4OO Tutorial

Use the AS4OO on-line tutorial to "round out" your AS4OO knowledge. Although 40 hours is the recommended time for this you may get through much quicker depending on your computer knowledge and what you have picked up on the AS4OO this far.

AS4OO Help Facilities

The AS4OO has extensive on-line help facilities. Additionally you will find the Search Index Command facility useful. This gives brief "how-to-do" summaries and definitions of terms. Suppose you have seen the term "object" and you do not know what it means:

* On the Command entry line of your screen key in STRIDXSCH and hit enter.

* When asked to type in a phrase or work, type OBJECT and enter.

* One of the listed entries is entitled "ABOUT OBJECTS".

* Move the cursor to that entry and type 5 and enter.

* A full screen definition of "OBJECT" will appear.

(Object is a much-used term, incidentally, and will be referred to with regard to security and backups.)

A full explanation of help and search index is at the front of manual SC21- 8083.

AS4OO Commands

* Positioning the cursor on the command line and pressing function key 4 will give you a structured list of available commands .

* Entering a command and pressing function key 4 will give you a prompt screen.

* If you want to display what options are available in a field on a prompt screen, move the cursor to the respective input field and hit the help key to get full help facilities or strike the "?" key to obtain a list of options.

AS4OO Standards

Instant Logic publish a book called "Standards for AS4OO Installations" which covers:

* General Naming Rules
* Abbreviation Rules
* Libraries
* Source Files
* Database Files
* Data Fields
* Security
* Communications
* Programming Standards

This may be useful after you have completed your top level audit reviews and want to delve into the efficient running of the AS4OO installation.

LEVEL 6 AUDITING

By now you will be an expert!

Construct audit routines and detailed audit tests to be performed on a regular basis.

Conclusion

In an article of this size only a summary can be presented. Nevertheless I hope that the tips shown will save you time when starting to audit the AS4OO .

The approach taken starts with a broad range of issues relatively thinly. This is intentional. The advantages are:-

* You have a good chance of exposing 80% of the major weaknesses with 20% of your time/effort.

* Future audits can be more closely defined.

* You will arrive at a better level of audit skill at a faster rate.

If you are in the comparatively luxurious situation of being able to go on one of the expensive courses specifically designed for audit of the AS4OO, you could still find it very useful to work through some of the material. By being more familiar with some of the concepts you will probably make better use of the course.

BIRMINGHAM MEETING

GOOD NEWS FOR OUR MEMBERS IN THE MIDLANDS

In a recent survey, some members asked for more meetings to be held outside London. So your committee chose three popular topics from our 1990/91 programme, for repetition at a full day meeting held in central Birmingham on September 27th 1991. The topics were "Risk-based audit planning", "CRAMM - an internal auditor's view", and "PC viruses". (Details of this first event for the 91/92 programme were circulated with the new programme cards in September.)

We arranged this as a joint meeting with the IIA-UK (Midlands District), whose other meetings BCS CASG members may attend as visitors. It has also been agreed that the IIA-UK (Midlands District) will join the BCS CASG as a corporate member, so that their members may attend BCS CASG meetings in London.

If these reciprocal arrangements prove to be successful, your committee will no doubt arrange other activities for out-of-London members.

Details of the IIA-UK (Midlands District) 1991/92 meetings have already been sent to all CASG members. They appear very broad ranging, with several of particular interest to computer auditors. Please note that most are half-day or full-day, that pre-booking is required, and that a small fee is payable in advance to cover costs, including refreshments. If you go to an IIA meeting be sure to let them know that you are a BCS CASG member, so that we can judge how popular the reciprocal arrangements are.

SOUND BYTE

MATCHING THE ROLE OF EDP AUDIT WITH THE NEEDS OF THE AUDIT COMITTEE

MALCOLM LINDSEY

Argos

No doubt many EDP auditors have wondered how their work shapes up to the expectations of the Audit Committee. At Argos, our audit department has a risk model which includes specific EDP audits. This is presented to the audit committee by the audit manager. The audit committee also receives copies of all completed EDP audit reports, which are as far as possible written in English rather than 'computer speak' ! So, in theory, communication should be fine.

We still had some nagging doubts:

- Did the audit committee understand the EDP audit function?

- Was there a way to obtain feedback so that their specific concerns could be addressed?

I concluded that if these questions were presented directly to the audit committee, there would be positive mutual benefits . With the support of the Audit Manager, I prepared a Presentation. The presentation covered the following areas (some specific details have been omitted for security reasons);

Objectives of Presentation

- To describe computer audit within Argos, and identify current strengths and weaknesses

- To elicit feedback during the presentation to focus computer audit work within the company

Computer Auditing Background

- Requires auditing and computing skills

- Three UK bodies:

  * IIA
  * BCS Computer Audit Specialist Group
  * EDPAA

Functions of Computer Audit

- Application control review

- Computer installation audits

- Disaster and contingency work

- Security reviews

- Technical reviews

- Computer assisted auditing

- Special projects

- Pre-implementation work

Strengths , Weaknesses , Opportunities and Threats

(Details of SWOTs for computer audit provided an excellent framework to describe the current status of the function, and provoked feedback for what the audit committee wanted in the future. These will vary from company to company; for obvious reasons, those of Argos are not listed!)

Computer Audit Work in 1990

(A handout was provided describing the areas covered.)

Conclusion

To provoke thought, the findings of the Computing/-Price Waterhouse survey of March 1991 was presented. This shows that 40% of respondents considered their major difficulty to be the integration of IT within corporate strategy.

My view is that computer audit is in an excellent position to "add value" by promoting the company perspective to IT professionals within the company. My presentation showed several 1990 audits where EDP audit had influenced computer projects from a business perspective .

Was it worthwhile? Judging from the feedback received and the comments from the committee, it was a useful and positive exercise.

THE AUDIT COMMISSION'S SURVEY OF COMPUTER FRAUD & ABUSE

CHRIS HURFORD

Associate Director at the Audit Commission

Since the early 1980s, the Audit Commission and its predecessor body has been undertaking triennial surveys into the extent of computer fraud and abuse within the UK generally. The intention of these surveys has been to:

- identify those aspects of computing which pose the greatest risks to the financial and administrative well-being of organisations;

- the Commission's client base in local government and the National Health Service in England and Wales; and

- provide an authoritative survey of UK computer fraud and abuse for the benefit of management and audit.

The most recent survey has now been published and provides a valuable insight into the most common types of computer crime affecting the public and private sectors within the UK. A wide range of questions was included in the survey form so that information could be gleaned on the nature of the incident; the perpetrator; the method of discovery; the action taken; and the reasons for the incidents occurring.

There is little doubt that accidental damage causes the most problems to the computing process and has the greatest impact upon the financial and administrative well-being of organisations. In the latest survey by the Audit Commission, 80% said that accidental acts posed a greater threat and this has been borne out by other surveys in Europe and North America. Unfortunately it is not possible to put a reliable figure upon the impact of accidental computer mishaps upon organisations. Losses through fire and flood can, for example, be quantified through insurance costs and the major problems caused by programming error are occasionally documented in the media but by far the larger part are known only within organisations where they occur and are rectified.

While accidental damage occurs more frequently, deliberate acts of computer abuse are, by their very nature, more sinister and should not be underestimated merely because they are perceived to represent a lesser share of the total threats to a computerised organisation. It is difficult too to put a figure on the total number or financial consequence of such actions and no-one can say with any certainty how much the UK economy loses through computer abuse. Indeed there is a reluctance in some quarters to disclose acts of computer abuse and some substantial losses are generally known to have been suffered by some organisations who, for their own reasons, have decided not to prosecute the case or to make information publicly available.

Claims are frequently made as to the extent of losses caused by computer fraud and abuse but they are rarely if ever substantiated and the Audit Commission survey does not purport to provide a definitive list of UK computer fraud and abuse incidents. Rather it provides an indication of the nature of the risks which organisations do face when relying upon technology to support their business activities. The survey draws too upon first-hand experience from those who have actually suffered incidents of computer fraud and abuse rather than conjecture and estimates and relates only to deliberate acts of fraud and particular types of abuse

The absence of any statutory obligation upon organisations to disclose acts of computer crime hampers any attempt to provide a reliable estimate of the extent of the abuse but it is sufficient perhaps to recognise that those activities which are known about are only the tip of the proverbial iceberg.

While too the Commission's survey provides details of the financial losses which have been suffered by some organisations, there could well have been far more devastating consequences of the incidents of fraud and abuse. Loss of information and of public confidence caused by the apparent ease which which individuals could hack into computer networks will be of concern to those dependent upon demonstrating the secuity of the data in their care.

Over 1500 organisations responded to the 1990 Survey and 180 incidents were reported with a total direct loss of over £1 million. Frauds accounted for 73 of the cases and there were 27 instances of theft, 26 hacking incidents and 54 virus attacks. In comparison with the results of previous surveys, frauds have continued to rise whilst other types of incidents have varied in frequency.

Of particular interest to management and audit, though, is the nature of the incident, how it occurred and whether it could have been prevented. Taking on board these messages should mean that readers may learn from others' experiences and install procedures which minimise losses in their own organisations.

Traditionally, the unauthorised alteration of data prior to inputting into the computer together with the alteration of computerised data accounted for the largest single number of fraud incidents. Within the cases reported from central government, three were input frauds, one was caused by the misappropriation of output and one involved the alteration of programs. The changed pattern of all the reported cases in the survey shows that output and program frauds now represent a larger share of the overall number of fraud cases although input frauds still dominate overall. There does not seem to be any particular reason for this shift in types of fraud but an increase in program frauds should give some cause for concern.

In comparison with the 1987 survey, there has been an increase in the number of expenditure, as opposed to income system frauds with more frauds being perpetrated through submission of unauthorised invoices and claims or the alteration of computerised payment data. The increasing dependence upon terminal-based systems to cope with claimants' payment systems makes such applications prone to fraud if safeguards are not built into the clerical and computerised processes. The absence of an adequate division of responsibilities with the onus being placed upon a single terminal operator to deal directly and wholly with claimants may at first sight seem efficient and cost-effective. The costs of that arrangement must be weighed against the risks of such an individual being able to create fictitious claimants' records and make payments through an automated payments system direct to a bank account.

As in 1987, most frauds were made possible by the absence of basic controls and safeguards. Often the lack of the "textbook" control provided the opportunity for the fraud to be perpetrated and knowing what the risks are and the incidence of such acts of computer abuse is important to management and to its auditors if precautions are to be taken. The adage 'prevention is better than cure' is particularly relevant as there is little doubt that the installation of adequate control and security measures would have prevented most of the reported incidents - and possibly help avoid the occurrence of the unreported acts, too.

Based upon the experience of having conducted four surveys over the past decade there are some consistent themes which, we believe, deserve the attention of management and auditors.

Few organisations seem to recognise that part of the cost of IT is its security and yet as desktop computing becomes an everyday part of business life so the need for better security measures will increase.

Because the cost of computing is falling many more staff are being given computing facilities to perform their daily tasks and yet comparatively few of them are given training in protecting the data on which they - and their employing organisations - rely.

With so many more users of microcomputers linked to networks, the need to ensure that access is restricted and controlled becomes more important.

Basic controls implemented successfully could reduce the exposure to risk.

Audit has a vital role to play in advising upon and helping to design controls and security measures but more computer-literate auditors are needed to help users and management appreciate the increasing risks which computing presents.

The **Survey of Computer Fraud & Abuse 1990** Report and a separate **Supplement** containing details of all the cases used in the survey analysis are both available from the Audit Commission, Nicholson House, Lime Kiln Close, Stoke Gifford, Bristol BS12 6SU.

The report is priced at £7.50 and the Supplement at £9.50 and cheques should be sent with orders.

Chris Hurford is an Associate Director at the Audit Commission and has responsibility for computing facilities within the Commission and computer auditing undertaken at clients. He has managed the production of all the fraud surveys.

SYSTEM DEVELOPMENT PROJECT MANAGEMENT
Part 1 - WHY DOES IT ALWAYS GO WRONG ?

VIRGINIA BRYANT

School of Informatics, The City University

System development projects frequently involve large amounts of resources and long time spans. Often the outcome is disappointing; projects are abandoned, or completed without providing a system which meets users' expectations. Some projects eventually limp to a close amidst disappointment and recrimination. Often the people involved move on. The resources at risk and the criticality to the enterprise, of the systems being developed, indicate a need for audit attention.

This article outlines the main problems encountered in managing the systems development process. The common problems identified are drawn from the experiences of nine project managers, and from recent survey into the management of information technology. These problems are discussed under the headings 'environment', 'planning' and 'methodological support'.

In Part 2, a second article on this theme to be published later, the role of audit in increasing the likelihood of development project success is examined.*(The incorporation of controls into the computer system being developed is viewed as a separate matter, and one which is not discussed here.)*

ENVIRONMENT

The environment in which system development projects are planned and carried out can result in a range of cultural/political problems which adversely affect these projects. Specifically;

Lack of Management Consensus

Two domains exist; the technology domain and the business domain. Systems are developed in the former, for (and with resources generated by) the latter. The management of the two domains have difficulty in communicating with each other because they have different backgrounds and objectives. Inadequate communication between the two domains leads to a lack of management consensus about what the project involves and what it will do. Multiple perspectives on this will exist; they need to be recognised and addressed. For example, 'information economics' (4) develops management consensus by requiring systematic focus by management in the two domains on aspects of the proposed project's contribution to the business and on its perceived riskiness arising from characteristics of both the proposed project and its environment. Managers are required to assess each information systems project proposal on a number of specific factors (Fig.1).

The technique uses worksheets which require managers to score the proposed project's impact on the business, by reference to a set of statements about the relationship between the project and factors in each of the two domains.

Fig.1. - 'Information Economics' - Categories for the Assessment of the Impact of a System Development Project.

In the business domain;

- Strategic Match
- Competitive Advantage
- Management Information
- Competitive Response
- Project or Organizational Risk

In the technology domain;

- Strategic IS Architecture
- Definitional Uncertainty
- Technical Uncertainty
- IS Infrastructure Risk

The results from this process, in terms of scores generated for project ranking purposes, may be less valuable than the management consensus built about the project's likely impact on the business.

Inappropriately Experienced Management

Technical training and experience are sometimes wrongly perceived as adequate preparation for project management responsibility. This can lead to poor performance and unfair criticism of project managers.

The assignment of staff without appropriate experience to project management, can adversely affect the manager's and the project team's moral. More careful selection of staff for project management and specific project management training is required, since a shortage of IT specialist staff was identified as the main problem in implementing IT projects by a recent study(1).

Confusion Over What Constitutes Control

Misunderstandings exist about what constitutes control over projects. Business management may apply pressure in the form of deadlines as a substitute for forms of control which require greater understanding of the project. Attempts to appear to be meeting deadlines can result in a lack of objectivity in the recording of data about the project by the project team. This results in the loss of true data about the progress of the project which could be used for future project planning. Real control requires real measurement. Without real measurement, real control is never obtained. The project estimation and project control functions need to be separated if reliable measurements and projections are to be established. (2)

If deadlines are used to give the illusion of control, all other measures become of secondary importance; attention is diverted from the real issues of cost and meeting user requirements.

Prioritisation

Different managers all believe that their department is the most important when determining the functions of any new system. Resolving user requirement priorities is a problem. Cross- functional systems can lead to conflict. Project proposal evaluation techniques which take an organisational view and assesses all proposals on a consistent basis, can be used to establish priorities and develop more robust plans. (Again a technique such as 'information economics' (4) could be useful here.)

PROJECT PLANNING PROCESS

Given that system development projects are relatively risky undertakings for most organisations, standards and guidelines on project planning and control can help; but there are other issues too;

Useful Models Needed

Project uniqueness requires project specific planning. This in turn depends on adequate models of the development process to provide a planning framework. Models in terms of activities, products, events and decisions, are needed to;

- assist understanding
- provide a framework for measurement and accounting; including size, cost and quality measurement.
- permit the integration of projects with other business activities.

TATE (7) argues that some of the problems in software development stem from the use of models that do not adequately reflect the development process and do not support the dynamic replanning that is a common feature of development work.

Time and Resource Projections

Project managers regularly under-estimate the times needed to complete various stages of a project and the project time itself. Allowances for training, meetings etc. are rarely adequately incorporated. DeMARCO (2) suggests that projections rather than estimates should be used wherever possible, and that a separate measurement group be responsible for all planning projections related to the project, but not for the work itself. The dispassionate judgment required to make reasonable estimates would be compromised by ego involvement in performance. To prevent adverse influencing of the estimates, the estimators should not report to anyone who has a stake in development. Success for the estimator must be defined as a function of convergence of the estimate to the actual.

Project control should be by reference to deliverables. The component activities of the project model are cost generators. A project activity is defined by its deliverable. There should be one activity per deliverable. The only work charged against that activity is work spent producing that deliverable. The activity is complete when the deliverable is delivered and accepted.

The complete project specification (project plan) ought to include the items shown in Fig.2.

Fig.2. - Contents of Project Specification

-activity network

- descriptions of deliverables
- set of detailed method descriptions, one for each primative activity
- timing of activities
- manpower requirements for each activity
- PERT or CPM analysis of critical paths
- tentative individual assignments

Risk and Contingencies

Plans should allow for what might go wrong and give indication of what to do if it does go wrong. Critical assumptions, information and decisions need identification so that when the plans change we can understand the effects of these changes. Plans must be available for all to see. Feedback is beneficial and planning is a communication tool too.

Control techniques such as Critical Path Analysis, where target start and completion dates are set for every development phase and task are also useful only

if progress is monitored by reference to deliverables, and if problems and delays, once identified, lead to dynamic replanning.

METHODOLOGICAL SUPPORT

Despite the growing awareness of system development methods and the development of prototypical approaches to system development, poor requirements capture processes still cause projects to fail. Inadequate definition of initial software requirements was identified as a major cause of difficulty in implementing IT projects by the survey (1), and was mentioned by most of the managers (5).

The use of an appropriate systems development method to guide the project team along the path of minimum time and cost, towards a reliable system, should assist. The specific objectives of a systems development methodology are to;

Ensure that systems are developed in a controlled manner with recognised review points, in order to reduce progressively the risk involved.

Provide an agreed framework for the joint development of systems by users and data processing.

Improve communication and commitment between the project group and the end users of the system.

Prevent duplication of effort.

Minimise documentation.

Provide a common terminology in systems development and serve as a reference for project staff.

The widespread use of software tools in the system development process means that there is often a considerable learning curve to cope with, whilst deadlines loom. The integration of these tools with other methods and the other tools used in a project often causes difficulty. The survey (1) found that only a quarter of the respondents used a project control method that is integrated with their system development method.

CONCLUSION

Project failure results mainly from management weakness; technical causes of project failure are very rare.

While project managers may claim to understand the process they are managing, the results suggest that we still have a long way to go before the system development process is sufficiently well understood for effective management. The reasons for project failure identified in practice, resulted from poor understanding about the environment in which the project is undertaken, and from a lack of useful models of the system development process to guide its managers.

Some environmental problems could be overcome by gaining management consensus about the impact of the project on the organisation as a whole, to develop cross-domain communication and to lead to better prioritisation of projects. Techniques which improve understanding about the impact of the proposed project on the business could be useful.

For project planning and control, 'deliverable' based project models which facilitate measurement and support dynamic replanning should be adopted.

While project managers are wiser in hindsight, quantification and modelling of what went wrong is rarely attempted. (Where the project progress data has been produced to show what the managers want it to show, such analysis may not even be possible.) How can we improve the process, if we do not learn the general lessons ?

Acknowledgement;*This article is based partly on a report by David Palmer of a meeting of The British Computer Society's North London Branch held on Wednesday 24th October at The London Business School. The three speakers were from; Hoskyns Group plc, (David Price), British Telecommunications plc (Dave Fursman) and Cranfield IT Institute.*

Bibliography and References

(1) BRYANT V., LEEMING A & WILLCOCKS L. (1991) Study of the Management of Information Technology (Forthcoming TCU Report)

(2) DeMARCO T. (1982) Controlling Software Projects (Yourdon Press)

(3) KUMAR (1990) Post Implementation Evaluation of Computer Based Information Systems - Current Practices (Communications of the ACM Vol3, No.2, pp203-212

(4) PARKER M. & BENSON R. (1988) Information Economics (Prentice Hall)

(5) SEWELL J. (1990) Methods for Determining System Development Risk: Evaluation of an Exposure Matrix (MSc. Project Report:TCU)

(6) SMYTH D. (1990) Keeping Control with Post Completion Audits Accountancy August pp163-164.

(7) TATE G. (1990) Process Models for Software Management (Internal:TCU)

(8) TRAVIS B (1987) Auditing the Development of Computing Systems (London:Butterworths)

THE COMPUTER AUDIT SPECIALIST GROUP OF THE BRITISH COMPUTER SOCIETY

INTRODUCTION

The Computer Audit Specialist Group is one of the oldest and largest of the British Computer Society's many Specialist Groups. The BCS is a charted institution with over 35,000 members and its Specialist Groups represent the many diverse areas of information technology.

The Computer Audit Specialist Group itself has wide ranging interests and these are reflected by its varied membership which comprises people from many professions including accounting, information technology, central & local government, banking, industry, computer security and academia.

The group has over 400 members and the top 100 companies are well represented.

GROUP OBJECTIVES

The objectives of the Group are:

a) To encourage research into information technology audit and promote the development of auditing and control techniques to reflect changes in technology, legislation and society.

b) To provide a forum for the development of awareness and competence in information technology audit.

c) To promote the efficient, effective and economical use of audit and control in the information technology environment.

d) To represent the interests of the Specialist Group to other bodies.

e) To be the primary focus for Audit and Control matters within the BCS.

The pattern of the Group's activities is organised by a Management Committee, which has a policy of evolution and of keeping in step with developments and current problems. On one hand the stability of the group is demonstrated by the fact that the 25 years have produced only four Chairmen, while on the other hand the Committee membership is subject to some change almost every year, when young blood and new ideas are introduced.

BENEFITS OF MEMBERSHIP

The benefits of membership can be summarised as:

* Quarterly Journal
* Monthly Meetings
* Annual Conference
* Discussion Group
* Magazine Discounts
* Meeting other people interested in the control, audit & security of Information Technology.

The annual subscription entitles the member to free attendance at the monthly meetings, a reduced admission rate for the annual conference, the opportunity to participate in discussion groups and reduced subscriptions to two international magazines: the **Computers & Security Bulletin** and the **Computer Fraud & Security Journal.**

The savings on the conference and magazines amount to many times the annual subscription, while the Group's own quarterly journal keeps members in touch with advances in control and audit techniques and with each other. The really big bonus however, is the opportunity to meet other people involved in the computer audit profession. A profession which is gaining in importance as it is recognised that control in computer applications and developments is often of critical importance to the survival of an organisation.

THE MONTHLY MEETINGS

The Group's season runs from October through to May with monthly meetings which are usually held in central London. Most meetings commence in the late afternoon at 16.30 with tea and biscuits available from 16.00, so that members have a chance to discuss mutual topics of interest with their colleagues before the meeting starts. An exception is the half day meeting which commences at 13.30.

The programme of meetings is specially tailored to reflect the diverse interests of the membership, but with a strong emphasis on computer audit and security matters.

Each meeting is addressed by at least one speaker and there is an informal get together afterwards, where sandwiches are supplied to soak up the more traditional liquid form of refreshment which many computer auditors seem to prefer!

The programme of monthly meetings is given in the annual programme card which you will find included with this information package.

DISCUSSION GROUP

The Discussion Group meets twice a year and the topics often follow-on from a theme established at one of our late afternoon meetings. These meetings are usually addressed by four speakers and attendance is limited to ensure that discussion really does take place.

ANNUAL CONFERENCE

The Group is well known for tackling the control and audit implications associated with new technologies and its annual conference is recognised for dealing with advanced subjects. Recent conferences have included the Control and Audit of Database, Expert Systems, Computer Aided Software Engineering, The 1990's - Concerns & Opportunities and Building Successful Business Systems.

Non-members attending the conference pay a higher rate than members, but this entitles them to membership of the Group for a year. The conference is thus used to promote membership of the Group and the BCS.

PUBLICATIONS

One of the Group's primary roles is the transfer of knowledge on audit and control techniques to other bodies and a number of publications have been produced to help achieve this aim.

Titles include:

Buying Payroll Software

Buying Financial Accounting Software

Buying Stock Control Software

Buying Sales Order Processing Software

Control and Audit of Database

This last publication was prepared in conjunction with the Data Management and Computer Security Specialist Groups of the Society.

To a certain extent this co-operation reflects the advantages of being affiliated to the BCS. If you have a particular hardware, software, security, audit, or control problem, then you can usually find help from one of the other Specialist Groups.

ANNUAL SUBSCRIPTION

The annual subscription comprises a multi-level rate to cater for individual and company needs and you will find the latest rates in the insert with this pack. The three levels of membership are:

* Corporate (Up to 5 named individuals)
* Individual (Not a member of the BCS)
* Individual (A Member of the BCS)

Corporate Membership

This allows up to 5 named individuals to be on the Group's mailing list and for 5 people from the organisation to attend the late afternoon meetings and to receive the conference discount.

Individual Membership

Under the guidelines of the BCS we are required to give a discount to those people who are members of the BCS and this is reflected in our separate rates for individual membership. An individual member will receive all the Group's mailings and is entitled to all the other benefits of membership, including free attendance at our late afternoon meetings, discounts on the magazines mentioned earlier and a reduced fee for our annual conference.

JOINING THE GROUP

The Group welcomes anyone with an interest in the control, audit and security of Information Technology; you don't have to be an auditor to belong and many of our members are from the mainstream I.T. profession. If you are involved in system development, system security, or the running of a computer installation you will find something to interest you.

If you are interested in finding out more about this very active Group you should contact the Membership Secretary whose name you will find on the enclosed application form.

You are also welcome to attend any of our late afternoon meetings to look us over; totally without charge, or obligation. You have nothing to lose and everything to gain.

THE COMPUTER AUDIT SPECIALIST GROUP OF THE BRITISH COMPUTER SOCIETY

CONSTITUTION

1. NAME

The Group shall be called the Computer Audit Specialist Group of the British Computer Society.

2. OBJECTIVES

a) To encourage research into the audit of information technology and promote the development of auditing and control techniques to reflect changes in technology, legislation and society.

b) To provide a forum for the development of awareness and competence in information technology audit.

c) To promote the efficient, effective and economical use of audit and control within information technology.

d) To represent the interests of the Computer Audit Specialist Group to other bodies.

e) To be the primary focus for audit and control matters within the BCS.

3. CONSTITUTION

The Computer Audit Specialist Group shall consist of:

a) The Officers, being Chairman, Secretary and Treasurer, all of whom should normally be members of the BCS.

b) Other officers to represent sub-groups or to perform other tasks which may be determined from time to time.

c) Individual fee paying members.

d) Corporate fee paying members, viz Companies, Groups or other organisations wishing to support the purpose of the Computer Audit Specialist Group.

4. ELECTED OFFICERS

a) The officers shall be elected by the Annual General Meeting (AGM) and shall serve from their time of appointment until the end of the AGM following.

b) A vacancy occurring during the term of office may be filled by an appointment by the Management Committee.

c) Other officers may be nominated to fill any other posts created by the Management Committee.

5. MANAGEMENT

a) The affairs of the Group shall be managed (subject to the control of the AGM) by a Management Committee comprising:

1) Elected officers

2) Co-opted officers

3) Elected members

b) Co-Option: the Management Committee may co-op members as required.

c) Meetings: The Management Committee shall meet at least four times in its year of office and frequently enough to properly carry out the business of the Group.

d) Notice: At least 14 days notice of the place, date and time of meeting shall be given to each member of the Management Committee.

e) Quorum: The business of the Management Committee may be transacted by not less then four members.

f) In the absence of the Chairman, the committee shall elect one of its number to take the chair for the meeting.

g) Voting: In determining a question by vote at a Management Meeting a simple majority will be sufficient. The chairman of the meeting shall have a second or casting vote if necessary.

h) Sub-Committees: The Management Committee may appoint at any time sub-committees with appropriate terms of reference, each responsible to the Management Committee and under the Chairmanship of a Management Committee member, to assist in carrying out the business of the Group.

i) Working parties: The Management Committee may set up at any time working parties responsible to the Management Committee which shall appoint a Chairman and provide appropriate terms of reference.

j) Branches: The Management Committee may set up at any time branches responsible to the Management Committee which shall appoint a Branch Chairman and provide appropriate terms of reference.

6. ANNUAL GENERAL MEETING

a) Each year the Group shall hold an AGM in May.

b) Notice: The Secretary shall send notice of the date, time and place of the AGM to all members of the Group at least 28 days before the Meeting.

For this purpose a notice printed in the Programme Card of the Group and complying with the above requirements shall be considered sufficient notice.

c) All members of the Group have the right to attend the AGM, for which there shall be no attendance charge.

d) Agenda: The following items shall be included:

1) Minutes of the previous AGM

2) Minutes of any Extraordinary General Meeting held since the previous AGM

3) Chairman's Report

4) Statement of Accounts

5) Proposals for alterations to the Constitution

6) Proposals for alterations to Fees

7) Election of Officers

8) Election of Auditors

e) Nominations: Any member is entitled to nominate a person for any elected office on the Management Committee. Such nominations may be proposed and seconded at the meeting if not previously received by the Secretary.

f) Voting: Every question at an AGM shall be decided by a simple majority of the votes cast. Individual members of the Group each have a single vote. The accredited representative of each corporate member also has a single vote. The chairman shall have a casting vote if necessary.

7. EXTRAORDINARY GENERAL MEETING

a) An Extraordinary General Meeting (EGM) shall be convened on a resolution of the Management Committee or within five weeks of receipt by the Secretary of a requisition signed by no less than twenty members (Corporate members having only a single vote) stating the business to be transacted at the meeting.

b) An EGM shall transact only such business as is specified in the resolutions or requisitions convening it.

8. FINANCE

a) Bank account: In accordance with BCS Guidelines, the Group shall have at least one Account (Account A) at Lloyds Bank, Langham Place Branch, used for normal running expenses. Other accounts at that branch or other places as approved by the Management Committee, may be used for special events or for investment funds.

b) the Group shall follow the BCS Financial Guidelines as issued from time to time.

c) The financial year shall start on 1st May each year.

d) The Treasurer is responsible to the BCS for submitting draft budgets, recording ongoing expenditure and capital expenditure separately for each by 30 November in the preceding year.

e) The Treasurer is responsible for making available to the BCS a revenue statement at the end of every financial year (30th April) in respect of the Group's normal operations and special events, this statement to be included in the BCS annual accounts subject to audit by the BCS auditors.

f) All cheques drawn on the Group's bank accounts must be signed by any two of Chairman, Secretary and Treasurer. In the event of such signatories being unavailable, then the Management Committee may appoint a member of the Committee to act as second signatory, together with one of the nominated signatories.

g) The accounts of the group shall be audited each year by an auditor elected at the AGM.

h) All income and property of the Group from whatever source derived shall be applied solely to the promotion of the objects of the Group.

9. DISSOLUTION

In the event of the winding up or dissolution of the Group any surplus assets remaining after discharge of liabilities shall automatically rest in the BCS.

In the event of an authorised officer of the Group not being available to conduct the transfer of any assets, then an appropriate officer of the BCS shall have the required power.

10. BRITISH COMPUTER SOCIETY

a) The Group shall be governed by the rules of the BCS as these apply to Specialist Groups of the BCS. Where it is considered that a rule of the Group is in conflict with a BCS rule governing Specialist Group activities, the BCS rule shall apply.

b) The Chairman of the Group must be a Fellow, Member or Associate Member of the BCS.

c) Other elected officers of the Group should normally be members of the BCS.

d) The Chairman, or other elected Committee Member of the Group, is ex officio a member of the BCS Specialist Groups Management Committee.

e) The Group must advise the Chairman of the Specialist Group's Management Committee of the names of any elected officers who are not members of the BCS.

f) All members of the Group's Management Committee shall abide by the Code of Conduct relating to members of the BCS.

g) The Group may use the BCS name to enhance the reputation of their own activities, but must not bring the BCS into disrepute.

h) No member of the Group may speak on behalf of the BCS without proper authority from the BCS.

PEOPLE

CHRIS BIRT

Chris read Economic History at the London School of Economics and then trained in local government to become a CIPFA accountant. He joined the City of London Corporation in 1984 and spent four years there as a computer auditor.

During his time at the Corporation he was involved in the entire range of computer audit work from installation security to systems development controls, from application controls to CAATs. He was also an active member of the CIPFA London Audit Group Computer Sub-Group, including chairing a working party which looked at a particular payroll package on behalf of the Group.

He is now a Senior Manager at Ernst & Young, specialising in Information Systems Audit and Security.

Chris is responsible for organising our Specialist Group's discussion days.

COURSES AND OTHER DATES OF INTEREST

This list has been prepared from material collected by several members of the editorial panel in the belief that some of these items may be of interest to CASG members. No reponsibility is accepted for the correctness of items. Further information should be sought from the event organisers whose details are given at the end of the list. Listing is free. If you have information about an event that may be of interest to members, please send details to; A.J. Thomas, 3 Kings Court, The Maltings, Great Dunmow, Essex, CM6 1UX.

TITLE	LEADER	DATE	LOCATION	ORGANISER
		1991		
Security and Audit of MVS/XA and MVS/ESA		30 Sept - 2 Oct	Amsterdam	Elsevier
Advanced Course in Internal Audit Report Writing		1 - 2 Oct	York	I.I.A.
MVS Audit, Control and Security Workshop		3-4 Oct.	Amsterdam	Elsevier
Managing Computer Audit		3-4 Oct.	London	I.I.A.
E.D.P.Auditing and Controls		7-9 Oct.	London	Elsevier
Audit and Security of LANS and Micro to Mainframe links		7-9 Oct.	London	Elsevier
Computer Security & Computer Audit		8-9 Oct.	London	C.I.P.F.A.
Computer Applications Audit - A methodology		8-9 Oct.	London	I.I.A.
Challenges for Audit Management		9 Oct.	Coventry	C.I.P.F.A.
Business Forecasting, Planning and		10-11 Oct.	Henley	Henley M.C.
COMPSEC - U. K. National Conference		30 Oct - 1 Nov	London	E.D.P.A.A.
Investigation of Computer Abuse	Mark Tantam	4-6 Nov	Oxford	Elsevier
Contingency Planning and Disaster Recovery	K.Pursall	4-6 Nov.	London	Elsevier
Audit, Control and Security of AS4OO and System 38		11-13 Nov.	London	Elsevier
Auditing a database Environment		12-13 Nov	London	I.I.A.
Heads of Internal Audit Seminar		12-13 Nov.	York	I.I.A.
Getting Your Point Across		13-14 Nov.	London	I.I.A.
Controlling Software Projects	Lister	13-15 Nov.	London	Niveau
Auditing in a Networking Environment		14-15 Nov.	London	I.I.A.
AS4OO and System 38 Workshop		14-15 Nov.	London	Elsevier
Project Management in the Information		18-19 Nov.	Henley	Henley M.C.
Systems Approach to Auditing		19-20 Nov.	Stratford Upon Avon	C.I.P.F.A.

TITLE	LEADER	DATE	LOCATION	ORGANISER
		1991		
Strategic Informations Systems Planning Management		20-21 Nov.	Henley	Henley M.C.
European Conference (6th)		20-22 Nov.	Paris	E.D.P.A.A.
Control and Audit of Relational Databases	E.McClements	21 Nov.	London	E.D.P.A.A.
Commonsense Computer Security	M.Smith	25-26 Nov.	London	Elsevier
MVS - Introduction, JCL and Utilities for Security and Audit		25-27 Nov	London	Elsevier
Computer Audit Workshop for Accountants and Auditors		25-29 Nov.	London	I.I.A.
Computer Audit Workshop for Professionals		25-29 Nov.	London	I.I.A.
Using SMF for Audit and Security		28-29 Nov.	London	Elsevier
Introduction to DEC VAX VMS Operating System		2-3 Dec.	Brussels	Elsevier
Advanced Computer Audit Workshop		2-6 Dec.	London	I.I.A.
Prevention & Detection of Fraud		4 Dec.	Solihull	C.I.P.F.A.
Advanced Audit, Control and Security of DEC VAX VMS		4-6 Dec.	Brussels	Elsevier
Measuring and Managing IT Benefits		9-10 Dec.	Henley	Henley M.C.
Internal Audit Manager's Course		9-11 Dec.	Horley	I.I.A.
Getting Most Value from your Spreadsheet		10-11 Dec.	Henley	Henley M.C.

Many of the above are courses or conferences charged at economic rates, but some are available at more modest charges. Fuller details may be obtained by contacting the organisers at the addresses listed below;

CHARTAC Courses and Conferences,ICAEW, 40 Bernard Street, London WC1N 1LD. Tel; 071 833 3291

CIPFA Courses by Courses and Conferences Unit, The Chartered Institute of Finance and Accountancy, 3, Robert Street, London, WC2N 6BH. Tel; 071 895 8823 (For Scotland 031 220 4316)

COMPSEC Courses organised by Elsevier Seminars, Mayfield House, Banbury Road, Oxford, DX2 7DH. Tel: 0865 512242

CPE Courses run by CPE Courses Ltd. Aldine House, Aldine Place, 142 Uxbridge Road, London Wl2 RAW Tel; 081 749 7467

EDPAA Meetings organised by the London Chapter of the E.D.P.Auditors Association. Enquiries to Stephen Bones of Neville Russell on 071 377 1000

ELSEVIER Enquiries to K. Russell, Elsevier Seminars, 256 Banbury Oxford, 0X2 7DH. Tel: 086S S12242

HENLEY M.C. Henley Information Technology Series Course organised by Hcnley,The Management College, Sharon Crabtree, Course Administrator, Greenlands, Henley on Thames, Oxon, R69 3AU. Tel: 0490 571454

IIA - Midlands District Society. Arrangements for individual meetings will be circulated to all Midlands District members in advance of each meeting. Members from other District Societies are welcome to attend but should inform the Secretary not later than 2 weeks before the meeting. (Secretary; R.O. Felton 0242 236111)

IIA(UK) Courses organised by the Institute of Internal Auditors (U.K.), Course Administrator, 13, Abbeville Mews, 88 Clapham Park Road, London SW4 7BX. Tel: 071 498 0101

MDC is the Management Development Centre, City University Business School, Frobisher Crescent, Barbican, London EC1Y 8HB Tel: 071 920 0111 ex. 2278 and 2359 or 071 374 0041 (direct line)

NCC National Computing Centre, Course Administrator, NCC, Oxford Road, Manchester, Ml 7ED. Tel: 061 228 6333.

DISCUSSION GROUP - AUDIT AUTOMATION

The next discussion group meets on **Wednesday October 30th,** at the Royal Institute of Public Health and Hygiene, 28m Portland Place, London W1N 4DE.

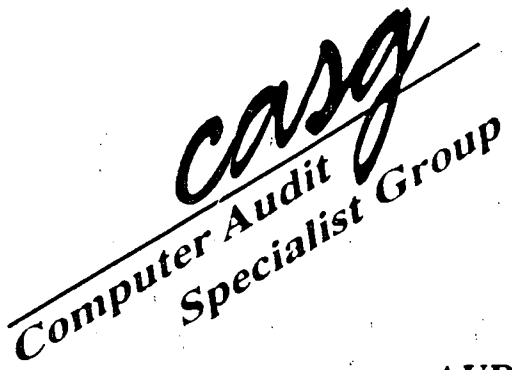
The purpose of the discussion is to enable us to exchange views and experiences and thereby enhance each others knowledge about Audit Automation. Therefore , the presentations are kept short and are meant to be thought-provoking, rahter than the definitive answer on each vof the four topics covered by our speakers.

If you would like to attend the day, please complete a booking form, (one is enclosed with this copy of the Journal), and return it to me, together with a cheque made payeable to BCS/CASG for #35.25 (including VAT). A receipt for, VAT purposes, will be supplied on request. The charge is being made to defray costs of the event, such as lunch.

Due to the nature of the day, numbers will be limited to 40. Places will be allocated as booking forms are received and I will write to confirm the allotment of a place or a position on the reserve list, as applicable. If you are subsequently unable to attend, please provide me with as much notice as possible so that your place can be offered to someone else.

I do hope you will be able to attend for what promises to be a most worthwhile day.

Chris Birt
Discussion Group Co-ordinator



The British Computer Society

AUDIT AUTOMATION

WEDNESDAY, OCTOBER 30, 1991

Time	Duration	Topic/Speaker
9.15 to 9.40	25 mins	Registration & Coffee
9.40 to 9.45	5 mins	Introduction
9.45 to 10.15	30 mins	Speaker from Ernst & Young's Audit Automation Group
10.15 to 10.55	40 mins	Discussion
10.50 to 11.10	15 mins	Coffee
11.10 to 11.40	30 mins	John Martin London Regional Transport
11.40 to 12.20	40 mins	Discussion
12.20 to 1.20	60 mins	Lunch
1.20 to 1.50	30 mins	Ian Read/Gordon Allan Bank of America
1.50 to 2.30	40 mins	Discussion
2.30 to 2.45	15 mins	Tea
2.45 to 3.15	30 mins	Andy Baruch Severn Trent Water
3.15 to 3.55	35 mins	Discussion
3.55 to 4.00	5 mins	Closing remarks

ABSTRACTS & BOOK REVIEWS

EXPERT SYSTEMS IN AUDITING

J.C. van Dijk and Paul Williams

Macmillan. £50.00. 224 pages

This is a book on the use by auditors of expert systems and not about how expert systems should be audited. It does therefore give only one side of the issue and that side itself is biased towards the external auditor; which is not surprising when it is realised that both authors work for BDO Binder Hamlyn. There are only three pages dealing specifically with internal audit, but again that is not surprising in view of the parallel nature of audit work regardless of the employment position of the auditor.

As with most books dealing in a new area, the early parts deal with the development of expert systems, the audit process and the potential application of expert systems to specific parts of the process. Indeed, it is not until nearly halfway through the book that we get to the nuts and bolts. If this sounds like a harsh criticism, it is not intended to be so. It simply reflects the fact that breaking new ground first requires establishing the starting position and then determining the direction and speed of travel. The remainder of the book follows the audit process fairly predictably through from initiation to completion, identifying the areas which are applicable to expert systems and giving examples of the systems which are currently available.

Well, what's my overall opinion? I found the book a useful introduction to the subject and it certainly mentioned a couple of systems of which I was unaware. Against this I have to consider that much of the book is really a description of the auditing process. Now we come to the real nub of the problem; who is the intended target audience? Auditors will already be aware of the main stages of the process and where expert systems could possibly help them, so what they need are detailed descriptions of the systems that are either currently available, or which are under development. On the other hand the developers will need to know about the audit process, so that they can fill some of the gaps.

I suspect that the authors had in mind the auditors, rather than the developers and the book does provide sufficient information about each of the systems mentioned to enable the reader to understand where and how it fits into the audit process. On the other hand much of the book explains what an auditor would already understand and this seems more suitable for potential developers. On balance it was an interesting read showing just how little down the road we are in applying these systems to the audit process.

John Mitchell

Read any good books or articles lately ?

If you have seen something that might be of interest to other CASG members please send details to;

"CASG Abstracts"
c/o Rob Melville,
Centre for Internal Auditing,
City University Business School,
Frobisher Crescent,
Barbican Centre,
London EC2Y 8HB.

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
MONTHLY MEETINGS	John Bevan	Audit and Computer Security Services	(0992) 582439
	Alison Webb	Independent Consultant	0223 461316
JOINT CONFERENCE ORGANISERS	Ian Longbon	CWB Limited	(071) 220 8495
	John Pringle	Department of Energy	(071) 273 0730
DISCUSSION GROUPS	Chris Birt	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
PLANNING	Bill Barton	The Rank Organisation Plc	(071) 706 1111
EDITORS, GROUP JOURNAL	Rob Melville	City University	(071) 920 0111
	Virginia Bryant	City University	(071) 253 4399 ex 3423

CONTENTS

DIARY		Front
EDITORIAL		1
CHAIRMAN'S CORNER		2
CHAIRMAN'S ANNUAL REPORT	John Mitchell	3
WHAT'S A CONTROL, DAD ?	Philip Weights	6
AUDITING THE IBM AS400	Malcolm Lindsey	8
SOUND BYTES	Malcolm Lindsey	13
THE AUDIT COMMISSION'S SURVEY OF COMPUTER FRAUD AND ABUSE	Chris Hurford	14
PROJECT MANAGEMENT WHY DOES IT ALWAYS GO WRONG ?	Virginia Bryant	16
ABOUT THE GROUP	John Mitchell	19
NEW CASG CONSTITUTION		21
PEOPLE	Chris Birt	23
COURSES & DATES OF INTEREST		24
DISCUSSION GROUP - AUDIT AUTOMATION	(Timetable)	27
ABSTRACTS & BOOK REVIEWS		28
MANAGEMENT COMMITTEE		Inside Back
VENUE FOR MONTHLY MEETINGS		Back

VENUE FOR MEMBERS' MEETINGS