Computer Audit Specialist Group

John D Bevan
46 Queens Road
HERTFORD
SG13 8AZ
Tel: 0992-582439

ISSN 0961-9348

The British Computer Society

JOURNAL

WINTER 1990\1991

Volume 1, Number 4

MEMBERS' MEETINGS FOR 1990/91

12 Feb 1991	4.00pm for 4.30pm	**Auditing the MVS OS**	Alan Oliphant *Standard Life Assurance*	KPMG Training Centre
12 Mar1991	1.30pm for 2.00pm	**COMPUTER ABUSE** (Half-Day Meeting)	Chris Hurford *Audit Commission* Sandy Douglas *Buxton Douglas Partnership*	KPMG Training Centre
27 Mar 1991	9.00am	Discussion Group **MAINFRAME ACCESS SECURITY PACKAGES**	Greg O'Shea *KPMG Peat Marwick McLintock*	KPMG Training Centre
9 Apr 1991	4.00pm for 4.30pm	**IBM's DB2 RELATIONAL DATABASE**	An IBM speaker	KPMG Training Centre
15 May 1991	9.00am	**ANNUAL CONFERENCE** **Building Successful Business Systems**		London International Press Centre
		User and Audit Responsibilities	Joe Hegarty *Surrey County Council*	
		Systems Controls	Peter Morriss *KPMG Peat Marwick McLintock*	
		Project Management and Control	Stuart Senior *Coopers Lybrand Deloitte*	
		Going Live and After Implementation	Chris Carr *National Audit Office*	
15 May 1991	4.30pm	**ANNUAL GENERAL MEETING**		London International Press Centre

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

EDITORIAL

SYSTEMS THINKING ?

Do systems' analysts and auditor's talk to each other ? How aware are they of each other's existence, specialism and role ? These questions have been brought to my mind recently. I was reading the Institute's IT Statement No.2 "Good Accounting Software" again, prior to expounding its salient points to some systems' analysis students, when I noticed that it makes no mention of the term "systems' analyst" anywhere in its 68 paragraphs. (Or in the useful questionnaire that comes with it) Perhaps this is because accountants and others are suspicious of letting systems' analysts get involved, less a perfectly adequate packaged software solution be overlooked by systems' analysts keen to develop software in-house (how else can the systems' analysts justify the purchase of that latest CASE tool!)

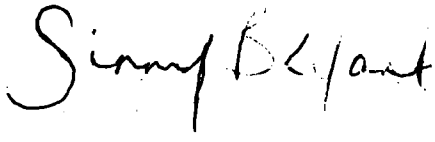
A few days later I was talking with a group of 30 part-time MSc. systems' analysis students. These people work in the daytime (mostly as either programmers or systems' analysts) and study here in the evenings. One of them was telling the rest of us about being hassled by "the auditors". Apparently the auditors had come in early one morning and removed all the diskettes they found on peoples desks, sitting in drives, etc.. When the systems' analysts and programmers arrived they found notes stuck to their terminals explaining that the diskettes had been removed as part of an audit exercise. I asked the group for suggestions about why the auditors had done this. "To check what was on the diskettes", was the reply.

This year's CASG annual conference will focus on "Building Successful Business Systems", thereby providing a focus for some valuable exchanges of ideas between systems' analysts and auditors. There appears to be a need for both groups to explain their side of things to the others.

OVER TO YOU ROB !

It has been a pleasure to work with members of CASG on starting up this journal. My special thanks to those people who wrote pieces in response to my phone call 'out-of-the-blue'. I was also very pleased with the response to invitations to join the CASG editorial panel. We now have a structure in place to enable the journal to develop further. Notably, Deborah Ashton has agreed to co-ordinate the production of future issues and Fred Thomas is preparing the diary sections. Philip Weights, Bryan Roche, Malcolm Lindsey, Fred Thomas, Brian Wallis and Rob Melville have agreed to scan various publications and pass on the interesting bits to the rest of us. Specific areas of interest, too numerous to list here, are being covered by panel members with relevant experience who will write and/or obtain articles for the journal.

Having produced the first four issues, I am handing over the editor's hat to Rob Melville. Until we can find someone to take it over, I will continue to do the DTP work. I'll assist elsewhere as necessary; and now that I don't have to do everything else as well, I've no excuse for not writing that article on "the support provided by systems' development methodologies for controls identification and specification", have I ?



CHAIRMAN'S CORNER

JOHN MITCHELL

During the Christmas period I was lucky enough to do a combined business/pleasure trip to Australia where I spent a couple of days with Graham Collier. Many of you will remember Graham who was secretary of the committee for many years before getting married and emigrating down-under about eighteen months ago. Graham is now Computer Audit Partner at Peat Marwick's Melbourne office and has become a father to boot (he blames it on the sun). Young Jennifer Pamela is proving more of a handful than a combined MVS/DB2 audit, but Graham and Bronwyn still found time to show me around their lovely city and to see a production of "A Midsummers Nights Dream" in the central park. As the moon rose over the lake, the local fruit bats (as big as crows) flew silently across it. It was a magic, if somewhat disturbing experience in view of the play's subject matter and Graham told me afterwards that he was sure that I had turned into an ass at that moment. To which I could only answer "not until then?".

However, nostalgia isn't what it used to be so let us move on to other matters.

Firstly, airport security. As an auditor with an interest in control systems I was particularly impressed with the security at Heathrow airport, where I was virtually body searched after the metal detector buzzed as I went through. I also noticed that the operative at the X-Ray machine was carefully examining every bag that passed through. Compare this with Singapore where I changed aircraft: the metal detector did not single me out, despite the fact that I was carrying the same things in my pocket as at Heathrow, and the X-Ray operative was paying scant attention to the screen; a situation which was to be repeated later at Sydney airport. Oh for an expert system whose attention would not lapse when doing such a boring, repetitive task.

Secondly, you will notice in this edition of the journal details of the editorial panel for "The Sweeper". Ginny Bryant has now managed to mobilise her volunteers, but this doesn't absolve the rest of you from doing nothing. A journal needs material and to a large extent we are relying on you to supply it. Please contact the appropriate member of the editorial panel if you have anything to offer.

On another matter have you looked at the new Computer Misuse Act? The drafters have been very careful not to define in detail what a computer actually is and although I can see the sense behind this, in view of the advances in technology, it does mean that each case will be unique in that it will first be necessary to establish if the "computer" concerned will actually be accepted as such by the court. From a personal point of view it now seems that the next time my niece re-programs my video recorder without my permission so that I miss that special program that I wanted to see, I can now prosecute her through the courts rather than resorting to the normal physical violence. Well that's some sort of progress I suppose!

Seriously though, if you are interested in the legal aspects of computing then I suggest that you come along to our half day meeting on the 12th March where Sandy Douglas will be providing one of his sideways looks at the subject and Chris Hurford will be reporting on the results of the Audit Commission's latest survey on computer abuse in the UK.

Now a plug for our annual conference for which you will find an application form with the journal. I am still amazed at how badly organisations manage the development process and how little impact internal audit seems to have from a practical point of view on the final system. Here is your chance to hear how it should be done, so come along and listen to the experts. It's still one of the cheapest conferences in the annual calendar and you will meet other members with problems similar to your own.

Finally, I would like to express my thanks to Stephen Crowe who has been a long serving member of your committee with responsibility for Discussion Groups. Stephen has been given vastly more onerous duties within Ernst & Young (it's called promotion) and has had to reluctantly give up his committee responsibilities. A great loss to us all. Best of luck for the future Stephen and a welcome to Chris Birt who has volunteered to take Stephen's place.

A DAY IN THE LIFE OF AN EDP AUDITOR

PHILIP WEIGHTS, Director European Computer Audit for a Swiss based banking group.

When I was asked by Virginia Bryant, Editor of the CASG Journal to contribute an article to the journal, I decided the easiest way to respond would be to simply document a day's work. This is it.

9am Arrive work. Read mail. Computer Weekly (Dec 6, 1990) has something interesting on the risks involved in the transfer of VISA credit card data. Barclays Bank, who process TSB Trustcards, sends tapes to TSB using a motorbike courier service. Seems like one tape fell off the back of the bike on the M25 and was crushed by a passing truck. Sounds like a case of data compression.

9.30 The financial auditors have requested a year-end recalculation of interest accruals using audit software. This is to satisfy the external auditors, KPMG, of the integrity of the data, and provide a basis for reliance on the balance sheet figures. The calculations will be performed for all deposits, including money market and fiduciary.

10.00 Where did I put the list of database files (actually dataviews in the jargon of the EDP dept.). Here we are, the files MMDEPO and FDDEPO need to be accessed to get the field descriptions, length and type. The mainframe is an IBM 3090 running MVS and Computer Associates DR/Datacomm database system. Via Data-Query I can print off the record layouts which give the fields needed to perform the interest calculations. As all good auditors and accountants know, the basic formula is as follows;

Interest = Principal * Rate * Time Period

This job looks easy.

11.00 Now the data has been downloaded from the IBM mainframe to my Toshiba laptop (T3200 1 meg CPU, 40 meg hard disk) using PC/Datacom. I've already determined the deposit start and end dates (value and maturity in banking terms) are stored in numeric format on the IBM 3090. So I can't simply subtract one from the other to get the nunber of days duration of the deposit. The dates must be first converted into Julian format. This can be achieved by exporting from PC/Datacom in DBASE III + format, and then importing this file into IDEA (audit software from the Canadian Institute of Chartered Accountants).

12.00 Here we go. Mathematical function, use the numeric DTVAL as source field, and create an 8 byte character field DTVAL8. Now we use the date conversion option to create the 7 byte numeric Julian date field called VALJUL, using DTVAL8 as the source field and masking the field as follows - XXYYMMDD. This is fun. Now let's do the same for the maturity date, and then create a new field with the Julian date for the audit date. All that remains is to apply the mathematical formula to compute the interest accrual, and then generate totals by different currency, and we're in business. While we are at it, in addition to the accruals, we can also check the full amount of interest computation through to maturity. Great.

13.00 The Toshiba is still chugging along merrily, but it looks like it is going to take a couple of hours to finish the calculation of interest for 6,500 currency deposits. Guess I'll grab a sandwich and catch up on my technical reading.

13.30 Hmm, Accountancy Magazine Jan 1991 has an interesting article on unauthorized computer entry. In a recent case, Denco Ltd. v Joinson, the Employment Appeal Tribunal decided that an employee who uses an unauthorised password to gain access to a computer containing information to which he or she is not entitled, is guilty of gross misconduct and can be summarily dismissed. If this was applied consistently in every instance, we would probably lose more than 50% of our DP staff.

14.00 How you doing Tosh, nearly finished. Let's take a look at some of the interest results and compare them to the detailed mainframe computer printout. With yellow and pink highlighters in hand, we set happily along, ticking and checking. Not very 'high tech' but necessary. Oh gloom and doom - a 50 % error rate, hot flush, panic attack, where do we go from here.

14.30 Back to the file layout. What's this field CDINTEMO? A two byte character field that can be any combination of 5, 0, or E (ie 55, E5, 05 etc). Nine possible combinations. Ah yes, some countries, have a different basis for calculating interest. There can be 365 day years, 360 day years (12 30day months), and exact years (366 in leap years).

15.00 Back to good old unreliable DBASE III + for some quick programming. Plenty of DO WHILE and DO CASE statements. Now fingers crossed, while exporting the file once more from IDEA

into DBASE format.

16.00 The new program is popping along but likely to take forever. Time to abort and call in the CLIPPER compiler. What is the syntax again for this, CLIPPER DEPOINT, then PLINK86 FI DEPOINT, NDX LIB CLIPPER. OK, another l0 minutes lost, but here we go again.

16.30 While the compiled program is finishing off I'll take a peek at the new book that just arrived called "Breakdowns in Computer Security" (Computer Weekly/PA Consulting Group). A bit skimpy for the price (£l3. 95 for 100 pages), but gives a good list of incidents occurring during the past two years. Example, October 1989 - A London bank (Citibank I recall) operated its APACS computer-based payment system twice in one day and transmitted £2 billion in duplicate payments. Why couldn't Barclays do that with my payroll cheque?

17.00Now printing the interest results again. This time it looks more encouraging. US dollars agree to the G/L, so do Swiss Francs, and £ sterling. OK that's good enough for me. Time to document the audit steps, the software developed, and the results obtained. That way KPMG will sign-off on the accruals. But look at the time, it's almost 6 o-clock. I guess documentation can wait until tomorrow,(Isn't that always the case?).

18.30 Final news item of the day appears during train ride from London Bridge. A London thief who snatched a laptop computer may have endangered battle plans for the Gulf war (according to USA Today Jan 8, 1991). This was viewed a serious security lapse on the part of a high-level British naval officer whose car was broken into. Hands up all you computer auditors with laptop computers who carry sensitive corporate data on trains and planes. This could happen to you, so be careful, it's a jungle out there.

DON'T FORGET THE ANNUAL CONFERENCE

This year's conference is on the topic of **Building Successful Business Systems** , and will be held on the l5th May 1991 at the London Press Centre.

Whenever anything goes wrong with a business system, the system is soon used as a scape-goat. In many cases it is a valid culprit, though this need not be so. To function properly a business needs a cohesive system as a workhorse for the enterprise. To achieve this the system must be properly designed and controlled, whilst at the same time giving users what they want.

The conference will look at some of the key issues which should be considered when constructing a new computer system. Some of the common pitfalls encountered will be discussed in order to point the way to achieving an easier transition to a successful business system.

Conference speakers have been drawn from commerce, local and central government, and from the audit profession. There will be ample opportunity to raise questions and discuss, including a panel session at the end of the day.

Admission fee, which includes conference papers, lunch and coffee is £138 for CASG or BCS members and £188 for others.

The outline programme for the Conference is shown on the front page of this issue. A more descriptive leaflet, including an application form, is being circulated with the journal.

Further information can be obtained by telephoning Ian Longbon's Secretary on (071) 623 8711 Extension 8711.

Admission applications will be dealt with in strict order of receipt by the Hon. Treasurer, and early application is advised.

RISK ANALYSIS IN AUDIT PLANNING

JOHN MITCHELL, PhD, MBA, MIIA, CISA, MBCS, MBIM

This paper is a synopsis of a presentation made by John to the joint meeting with the IIA on the 16th January.

INTRODUCTION

This paper deals with the subject of using risk analysis for audit planning purposes from a practical as well as a theoretical framework. On the theoretical side, most of the work was undertaken as part of the research for a PhD; on the practical side the author has worked at a senior level in two very large audit departments and as a consultant has knowledge of the planning processes of many others. This has provided first hand experience of the problems of planning audit coverage when faced with almost unlimited demands, but only limited resources.

THE PROBLEM AREA

In most organisations Internal Audit is an independent appraisal function for the review of operations as a service to all levels of management.

Internal Audit is a service function and is therefore, an overhead to the organisation. As such, it should have a clear methodology for allocating its resources to the most important areas of the business. This requirement arises because of the virtually infinite variety of work available to Internal Audit in contrast to its limited resources and the need for it to be cost effective in the use of those scarce resources.

THE RATIONAL AUDIT MANAGER

If an Internal Audit Manager were able to select his projects and allocate his resources entirely free of other direction, he would, in theory, select those areas for examination which he perceives as being of most importance to the business. He would then allocate his available and potential resources on the basis of this perceived importance. The allocation would be conducted on a totally logical and objective basis, which would be based on set criteria, or formulae, which could be applied consistently to all the different areas of the business.

In reality this allocation will itself probably be made on a combination of objective and subjective criteria, which will depend on the Manager's knowledge, or lack of knowledge, of each area and his personal idiosyncrasies. The Manager will probably find it difficult to explain to a non-auditor why he has chosen a particular area for review, why he has allocated a certain amount of resource, or indeed why he considers the need to do some of the directed projects as a waste of valuable resource.

Internal Audit planning therefore requires the balancing of the work to be done against the available resources. Effective and efficient audit is only likely to be achieved if operations are planned on a methodical basis, which highlights priorities and the allocation of resources.

RATIONAL PLANNING

Until recently, the establishment of priorities and the allocation of resources has largely been a matter of intuition, judgement and local knowledge but, as with all exercises involving judgement, important factors may be overlooked. Consequently, some Internal Audit Departments have devised so called "risk indices" which help to establish priorities on a more formal basis.

These indices involve an analysis of particular factors by formulating a set of values to replace what has previously been determined by intuitive judgements. Although the creation of such indices goes some way towards justifying why an Internal Audit Department examines some areas at the expense of others, they seldom go beyond the step of allocating priorities.

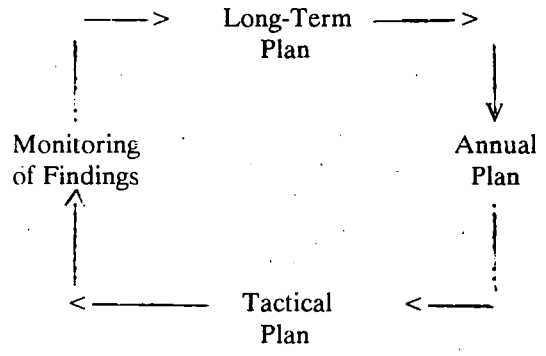
A comprehensive and effective planning aid should be capable of far more than the simple allocation of priorities. It should at least be capable of suggesting tactical resource planning for a single audit and ideally it should be capable of helping with the annual and long-term planning process. Just as importantly, it should clearly indicate those areas which will not be covered; either because they are considered to be of low importance, or because the resources are not available.

THE ROLE OF HISTORIC DATA

It is difficult to conceive of any business planning which does not to some degree utilise past data, even though there may be dangers in using the past when attempting to anticipate the future. The use of past data is of special significance to Audit Managers however, as they are often required to cover all major business areas, or units, in a particular time scale. In order to ensure that this coverage is achieved they need to keep records of what was done previously and to take due regard of previous findings.

From the above it can be seen that there is a relationship between audit planning and the findings from previous work and this is illustrated by the schematic below.

Planning & Monitoring Relationship



Any planning system must have the ability therefore, to record what work has been done previously and the results from that work. From this we can see that a planning system without its monitoring partner is unlikely to be fully useful to a manager.

HOW IMPORTANT IS THE FORMULA ?

Much has been written regarding the applicability, or otherwise, of various formulae. Many authors seem to see the formula as an end in itself, rather than as the beginning of the planning process. If the formula is correct, then everything else will then be okay appears to be the attitude of the formula proponents. Most authors admit however, that their formula might not be ideal for all purposes and some go even further and suggest that in the final analysis the judgement of the auditor is the most important factor of all. Just how important then is the formula in the planning process?

A survey of audit managers, who use risk analysis techniques for planning, revealed that they all used their own judgement in preparing the final plan. Although the majority had found the process useful in formulating their plan, they had all found that no formula could totally satisfy their requirements to produce a complete plan, as some of their activities had to be scheduled at the direction of top management. Thus the formula was an aid to planning and not a substitute for it. All the managers stated that the benefit came from the planning process itself and especially the data collection exercise.

The formula is really a catalyst which forces the auditor to collect data about the organisation he works for. Even if the data is not manipulated in a formal manner it provides a base line for the auditor to work on mentally. The advantage of manipulation is that it enables the auditor to question his own planning constructs and may even change the way he conducts the process in the future. Thus even if the formula is totally wrong it has helped the auditor to plan his work better.

DIFFERENT FORMULAE FOR DIFFERENT AREAS

The problem of deriving a formula which can be consistently applied to all areas of the business has defeated many audit managers. In order to overcome this problem they argue the case for using different formulae for different areas of the business.

At first sight this is an attractive proposition as it enables the best possible formula to be utilised in a particular area. Thus it is possible to rank all the (say) personnel projects one against another and all the finance projects against each other. The use of such a system produces a number of lists, one for each discrete area of the business, with projects ranked within each area. So far, so good, but what happens when an attempt is made to decide which of all the projects should be done first, or how much resource should be allocated for projects ranked the same, but within different lists? The situation facing the auditor is illustrated below.

Personnel	Finance	Stores
Project 1	Project 1	Project 1
Project 2	Project 2	Project 2
Project 3	Project 3	Project 3

Let us assume that the auditor has only sufficient resource to do two of the three premier ranking projects. Which does he do? They are all equally ranked, but are they truly equal? Does their equivalence really hold true? As different formulae were used to calculate them it is extremely unlikely that an individual element of (say) personnel risk equates exactly to a single element of stores risk. Does the auditor now need a mega-formula to determine which project should be eliminated? The answer is undoubtedly that he does. If such a mega-formula exists, then why not use it in the first place and do away with the individual formulae? But the reason that the individual formulae were required in the first place was because it was considered impossible to devise a single mega-formula!

The use of many different formulae also poses the problem of determining which formula should be applied if the project involves elements of each formula, such as stores and finance, as may well be the case.

DEFINING WHAT YOU ARE DOING

What is an Audit?

Many auditors describe an audit in the sense of a particular subject e.g. Payroll, Stores, Income, etc.,

but what does this really mean from the point of view of audit activity? One person's payroll audit is another's starters and leavers job. It is essential then that there should be some assurance that if the same audit were conducted by two different teams in two different locations, that exactly the same areas of internal control will be examined. This is especially important when comparing what is meant to be a similar activity between two different parts of a business.

What is a Location?

Although locations tend to be thought of as physical places it is conceivable, indeed likely, that certain operations from different divisions within a company will share the same physical place. If only physical locations were identified and recorded there is a possibility that apparently complete coverage could be achieved, in that all control objectives had been covered at a particular physical location, but in reality an important area could be overlooked, due to the location sharing situation.

What is a System?

Modern internal audit tends to use a system based approach to its work. In large organisations it is often impossible to define system boundaries and very unlikely that a complete system will be covered by a single audit. In order to cater for the diversity of operations encountered in a large company and to allow for the problem identified above, it may be useful to divide the company into Business Areas, such as Stores, Payroll, Marketing, etc. The advantage of dividing the business into well understood areas is that it is easier to ascertain how much resource is being given to a particular business activity. A Business Area should therefore be considered as an aggregation of like units of audit interest.

What is Full Coverage?

Although there is often a requirement to complete audit work in a particular time cycle, there is often no definition as to what is meant by this. Empirically it may be realised that some areas need to be covered more frequently than others, but which areas fall into each potential cycle within the maximum cycle? Indeed, should everything be reviewed at all? In view of most audit department's limited resources it may be more sensible to review those areas considered to be of greater importance on a more frequent basis, but at the expense of those considered less important.

PLANNING REQUIREMENTS

The following schematic indicates the major components of any planning system, whether it be manual, or computerised.

PLANNING SYSTEM COMPONENTS

COLLECTING THE DATA

The type and amount of data to be collected will obviously depend on the formula, or formulae, chosen by the auditor for calculating the importance score. If the formula has a large number of elements, or indeed just a small number of particularly exotic ones, it may prove impossible to collect all the necessary data items and assumptions may have to be made. Very few models can actually handle these unknown factors and it is only recently that expert systems have become available which can deal with uncertainty.

Many formulae examined by this author required more than 10 different items to be collected and one needed 28 items to produce a result. A formula with 10 items of data will often require 10, or more, separate calculations to arrive at a result, because of the various additions, multiplications and divisions required. In a large organisation there may be several thousand potential audit jobs which require to be analysed.

This in itself may not seem important if a computer is available, as it will be used to do the tedious work of calculation and recalculation. That is indeed the case, but for every item of data required for manipulation there is the problem and effort of collecting it in the first place and keeping it up-to-date in the second place.

If we assume a ten item formula and 5,000 potential audit jobs then we need to collect 50,000 items, for the computer to manipulate, with about 0.5 million calculations to be performed. Although this may be a useful job in its own right it is not a test to be undertaken lightly and the question of expending the effort of keeping it up to date also needs to be raised.

An example of a data collection sheet used by the author is shown below.

PLANNING SYSTEM INPUT

CODE: DESCRIPTION:

JOB TYPE (R/P): FREQ/YEAR (1-5): MUST REVIEW (Y/N):

DIVISION: DISTRICT/UNIT: CSA/LOCATION:

BUSINESS AREA: CONTROL OBJECTIVES: / / / / /

SIZE OF AREA (Millions): SIZE TYPE (A-E):

INTERNAL CONTROL (H/M/L/N): BUSINESS IMPACT (H/M/L/N):

TEMPTATION (H/M/L/N): AUDIT COMPLEXITY (H/M/L/):

LAST AUDITED (Year): REPORT NUMBER:

NOMINAL BUDGET (Days): TRAVELLING TIME (Days):

COMPLETION NOTES

CODE	: 4 digit numeric
DESCRIPTION	: 30 character description of the job
JOB TYPE	: Type of Job (R = Regulatory, P = Project)
FREQ/YEAR	: Year to be done for (P)roject jobs. Frequency of review for (R)egulatory jobs.
MUST REVIEW	: Must be reviewed regardless of score
DIVISION	: 3 Character Division code
DISTRICT/UNIT	: 3 character District/Unit code
CSA/LOCATION	: 3 character Customer Service Area
BUSINESS AREA	: 2 digit Business Area
OBJECTIVES	: Control Objectives
SIZE OF AREA	: The Total Value based on the type code
SIZE TYPE	: The "makeup" of the value A = Gross Asset Movements B = Income C = Expenditure D = Stores E = Wages)
INT. CONTROL	: H = Good/Satisfactory, M = Satisfactory except for ...., L = Unsatisfactory, N = Critical
BUS. IMPACT	: H = High M = Medium L = Low N = None
TEMPTATION	: H = High, M = Medium, L = Low, N = None
AUDIT COMPX	: H = High, M = Medium, L = Low
LAST AUDITED	: 2 digit year of last review
REPORT NUMBER	: 8 character report number
NOM. BUDGET	: Time required for the review (excluding travel) in days
TRAVEL TIME	: Time required for travel to/from job in days

KEEPING THE DATA CURRENT

In fact the problem of keeping the data current needs to be examined further. Some authors suggest that an annual exercise is all that is required. For a small department auditing a small number of jobs this may indeed be a suitable way of doing it. For a large department however the effort to collect and check say 5,000 items as an annual exercise is probably impossible due to time and resource constraints. How then can we ensure that we have the most up-to-date data for the planning process? The short answer is that unless we check the data just before calculation we cannot be certain of its currency. A large department is therefore faced with the problem of how much inaccuracy is it willing to bear in its planning process?

THE ROLE OF COMPUTER MODELLING

Computer modelling has been used for a number of years to aid management in planning for the future. Until fairly recently these models were limited in the business sphere to financial simulations on mainframe computers. The advent of powerful microcomputers and their associated software has enabled the modelling process to be conducted at a far lower level than was previously possible and even quite small parts of a business now use these tools for their planning process. The main area of planning still relates to financial affairs and the growth of comprehensive spreadsheet packages has reflected the requirement of management for more sophisticated planning tools.

Auditors were quick to appreciate the use of microcomputers to aid their audit work and it was the spreadsheet that introduced auditors to the usefulness of microcomputers as audit tools. Although originally used as a tool during, or after the audit, some audit departments used spreadsheet packages to do so called risk analysis exercises based on the many formulae that were being described by the various authors mentioned in a previous chapter.

This author has also conducted exercises of that nature, but has discovered that spreadsheets were not ideal for the planning process as they were generally cumbersome to manipulate, prone to user error and were often limited by the memory capacity of the machine, as they invariably required all the data to be held in memory.

USING A COMPUTER

The use of a computer system has the following advantages:

a) The individual projects can be held in a database which can be added to, amended and deleted from, as required;

b) The formula can be modified and applied to the database quickly and consistently;

c) Weights can be modified and tested in a similar way;

d) Results can be printed on hard-copy, or held in magnetic format, for subsequent comparison and analysis;

e) Data can be transferred between systems, thus facilitating the integration between the historic monitoring system and the planning system.

POTENTIAL PROBLEM AREAS

The following areas need to be considered before undertaking audit planning using risk analysis techniques:

(a) data collection problems;

(b) data validation requirements;

(c) the need for user friendliness;

(d) spreadsheet limitations;

(e) dealing with non-cyclical activity;

(f) the requirement to override low scoring jobs to force them into a particular year of the plan;

(g) the need to estimate a minimum cycle to ensure full coverage of the audit portfolio;

(h) the need for good definitions for 'audit', 'location', 'system' and 'full coverage';

(i) linking to any monitoring system already in existence;

(j) the difference between a subjective and a control objective approach.

RESEARCH FINDINGS

The main findings from the research conducted by this author can be summarised as:

a) Risk analysis, as applied to internal audit planning, is a misnomer. It would be more appropriate to describe the process as an analytical review across all potential jobs and to call the output from the process an "importance score", rather than a risk index;

b) The use of a formula to indicate the relative importance of a particular area to the auditor is practical;

c) If more than one formula is used to deal with different aspects of the business, then there is a danger that the auditor will be unable to rank items from one area against those of another area with any certainty of relative, or absolute merit;

d) The formula is not the most important part of a planning system;

e) The collection of the data to be manipulated by the formula is one of the most important aspects of the planning process, as it ensures that the auditor has a good understanding of the organisation he is responsible for;

f) The best time to collect the data required by the planning system is during an actual audit. This implies a link between the historic monitoring process and the future planning process.

g) There is no correlation between the importance of an area, as rated by its importance score, and the resource required to audit it;

h) There is a relationship between the complexity of the area to be audited and the resource that is required to do the work, but the relationship is not necessarily linear;

i) An "override" facility is required to ensure that items with a low importance score can be forced into the scheduling mechanism;

j) The data needs to collected at the job level if the system is to be capable of upward aggregation.

CONCLUSION

The use of standardised formulae to help with the audit planning process is not a new idea, but the use of low cost micro computers and the linking with a monitoring system makes it a far more potent tool than it has been in the past. This author's research has indicated that the data collection effort that is required should not be underestimated but it is this very collection of information about the organisation which enables the auditor to make sensible decisions about his coverage even if the data is not subsequently computerised.

DEADLINES FOR FUTURE EDITIONS

Edition	Submission Deadline
Winter	15th December
Spring	15th March
Summer	15th June
Autumn	15th September

Text in Wordstar or ASCII format on diskette preferred. Please send to; CASG Journal, c/o Rob Melville, Centre for Internal Auditing, City University Business School, Frobisher Crescent, Barbican Centre, London EC2Y 8HB.

CONTROLLING ACCESS CONTROL

JONATHAN D. MOFFETT
Imperial College, University of London

INTRODUCTION

This is a short report on the access control aspects of an academic project on the management of distributed systems. We have followed the principle of keeping our feet firmly on the ground while our heads are in the clouds. While much of our activity has been abstract and theoretical, there are a number of practical principles and lessons which are immediately applicable in the management of security in commercial data processing systems.

THE DOMINO PROJECT

The DOMINO project on Domain Management in Open Distributed System (technical director Morris Sloman of Imperial College) is a collaborative project funded by the U.K. Information Engineering Directorate, to last three years. It involves Imperial College, London, SEMA Group and the British Petroleum Research Centre. It is concerned with managing large scale distributed systems. One aspect of this has been the specification of discretionary access control policy and the delegation of access control authority in a way which gives flexibility while retaining management control. The overall aim of the project, currently at halfway point, is to implement a distributed system in which we can demonstrate a number of aspects of system management. The groundwork which we have carried out so far has already thrown light on a number of important principles for access control.

Large distributed processing systems have very large numbers of users and resource objects so that it is impractical to specify detailed access control policy in terms of individual objects or individual users. We need to be able to specify it as relationships between groups of users and groups of objects. The systems typically consist of multiple interconnected networks and span a number of different organisations. Authority cannot be delegated or imposed from one central point, but has to be negotiated between independent managers who wish to cooperate but who may have a very limited trust in each other. Protocols for sharing authority are therefore essential.

SOME BASIC CONCEPTS

Here are some of the basic concepts which underlie our work. None would make an auditor turn a hair, but we find that they are surprisingly unfamiliar to computer scientists.

Responsibility of Human Users

It is assumed that there are human users of the system, and that humans are ultimately responsible for the actions of the system. In many situations they will use automated agents to carry out this responsibility, but they will retain responsibility for the results, and are therefore required also to retain the power to control the agents.

Ownership

Ownership in computer systems is a concept as close as possible to normal legal ownership of goods and property. All computer systems in a country such as the UK process resources with identifiable legal owners who have legal powers over them. We regard ownership as the starting point for access control.

Most previous researchers have assumed that the user who creates an object automatically becomes its owner. We do not hold that view, but distinguish between ownership of objects and the delegated power to create them. A data processing clerk who submits a job to create a new file of bank accounts is not the owner of those accounts, but is carrying out the task of creating the file as an agent of the owner of the bank.

Authority

We define *authority* as the power which has been legitimately obtained. There are a number of ways in which legitimacy may be obtained, but for our purpose it is obtained in accordance with the currently applicable laws. We are concerned in our project with particular aspects of authority as applied to discretionary access control; with the means by which authority can be granted and removed dynamically; and with the delegation of these means within and between organisations in a controlled manner.

For the purpose of discussing authority we assume that we start with an owner, who can then dispose of or share his ownership or delegate a subset of his powers, to another person. Provided that this is done legitimately we describe this other person as having gained authority.

Delegation of Authority

Delegation of authority is an essential concept in large organisations, where the overall managers of the

organisation cannot possibly take responsibility at a detailed level. Managers need to be able to delegate authority to subordinates, who are given a defined subset of the manager's powers, to exercise in accordance with formal or informal policies. Delegation of authority must also be possible in computer systems. Therefore it is necessary to be able to identify the people (or positions) to which authority has been delegated and the powers they have been given. We have aimed in particular at defining these powers in the case of security administration

Negotiation of Authority

One distinctive factor in the management of distributed systems is that a distributed processing application may span the computer systems belonging to a number of different organisations, with no central authority. Authority cannot, therefore, be delegated or imposed from one central point, but has to be negotiated between independent managers who wish to cooperate but who may have a very limited trust in each other. They may wish to give each other access to their computer systems which is closely controlled both in the scope of the target objects which can be accessed and the operations which may be performed on them.

Separation of Responsibilities

Separation of responsibilities is an important control concept which is familiar in the context of auditing, but is seldom implemented in access control systems. One of our principles is that people responsible for granting access authority to system users should not be able to grant it to themselves. This requirement, in relation to Security Administrators, has been an important driving force in our work.

Global Access Authority

We make the assumption that there is no inherent right of access of any kind. If a person is not the owner of an object, and has not been given authority, then the computer system should refuse all access.

PRELIMINARY RESULTS

Separation of Responsibilities for Security Administrators

Our most important result to date is to show that it is possible to have a practical access control system in which the Security Administrators, while having the abililty to give access rights to other users, cannot obtain them for themselves. Surprisingly, the concepts and approach are straightforward, and separation of responsibilities for security administrators could be implemented on many commercial access control systems. The system owner (or authorised manager) delegates two kinds of authority to a Security Administrator, each delimited by a *scope*: his *User Scope* which defines the set of users to whon he can give access rights; and his *Object Scope* which defines the set of target objects, typically files, to which he can give users access. He cannot give access for users who are not within his user scope or to files which are not within his object scope. Thus we have a convenient mechanism by which owners and managers can define the limits of authority of a Security Administrator; for example a Marketing Manager can give him authority to make access rules for members of the Marketing Department to access Marketing files, in accordance with some policy which has been defined informally. Assuming he is not himself a member of the department, he cannot give himself access.

The real power of this mechanism comes with the realisation that, as a Security Administrator is not within his own User Scope, he cannot make access rules for his own benefit, and so our aim of Separation of Responsibilities is achieved. Of course, the Security Administrator has a legitimate need to access some files, and so a secondary Security Administrator is needed, with a User Scope which includes the primary one, to allow him access when necessary.

Negotiation between Independent Managers

The same mechanism, of scope of authority, can also be used to allow independent managers to negotiate the access which they are prepared to allow to outsiders, and alow that much and no more. Each manager has a defined scope of authority, in terms of both users and objects such as files, and he can delegate authority within these scopes, either to other autonomous managers or to their security administrators.

SOME PRACTICAL POINTS

There is not space to describe all that we have learnt, but here are some practical points which are directly applicable in commercial systems.

Domains for Grouping

It is quite impractical to deal with individuals for most access control policy decisions in large systems. If there are thousands of users and tens of thousands of files, then the only way to specify access decisions is by the access which groups of users can have to groups of files. We have used a special kind of object, a *domain*, as a means of grouping all kinds of objects into hierarchical structures. The equivalent of a domain can be found in many systems as a directory, a group or an organisational code associated with a user record. The same grouping principles which we have used with domains can be used with other structures instead.

Access for Positions, not People

If a named person is given access then when he changes his position, it is necessary to change the access rules to remove the access rights which were appropriate for his old position and create those for his new position. If, on the other hand, the access rights are given to a position, then they apply to the current occupier of the position and there is no need to change them when the occupier changes. This is probably the most important principle to follow in the practical administration of a large access control system.

We achieve this by representing positions as domains which users move in and out of as they occupy and leave positions, and then giving access rights to the domains rather than to the people. However, most commercial access control systems allow this principle to be implemented using their facilities for grouping users.

Ownership

The specification of our system forces every object to have an owner, and completely divorces ownership from creation. Both of these principles can be enforced by administrative means in any computer system.

Delegation of Authority

We have integrated the concept of delegation of authority from owners, through managers to security administrators, into our system. Even if these concpets are not integrated in an access control system they can be implemented administratively.

Removal of Access

Since we assume that there is no inherent right of access, the separate concept of taking action to prevent access need not arise; no-one has access unless it has been authorised, and the removal of that authorisation is sufficient to prevent access.

We have rejected the concept of negative access rights on both practical and theoretical grounds. Our observation of their practical use in large systems has been that it becomes very difficult indeed to decide on the actual effect of a mixture of positive and negative access rules. And it is possible to show that in some systems using negative rights it is possible to reach a self-contradictory position which can only be resolved by restating the requirements in positive terms.

We believe that negative rights - the explicit prevention of access, rather than the removal of previously granted authority - should not be used in security administration. The rescinding of previously made positive decisions to grant access is almost always the correct approach to the removal of access. An emergency requirement to deny access to a user can be dealt with by suspension of the user himself.

CONCLUSIONS

We have reached our practical conclusions by what might seem to be a very theoretical approach: specification using the formal specification language Z, use of the Prolog logic programming language to validate our specification with a small scale prototype and use of object oriented concepts - our implementation will be partly in Smalltalk-80 and partly in C++. However, the benefit of an approach which might seem a luxury to many commercial system managers is that we have a very clean design and are confident in the success of our implementation.

The project has some way to go. We are now starting design and prototyping of a system based on our specification, in order to demonstrate its viability on a small scale and gain enough experience to estimate how it will work on a large scale. We hope, in 1992, to show the success of our concepts.

The author will be pleased to give more information to anyone who is interested. He can be contacted at;

Department of Computing,
Imperial College,
Universtiy of London
180 Queen's Gate,
London SW7 2BZ

Email: jdm@uk.ac.ic.doc
Telephone: 071 589 5111 ex.5092

TOPICS FOR MONTHLY MEMBERS' MEETINGS

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

PRACTICAL PROBLEMS OF INTERNAL AUDIT INVOLVEMENT IN MAJOR SYSTEM DEVELOPMENTS - AND SOME SOLUTIONS

By JOHN NYE MA(Oxon), FCCA, MIIA, Systems & Computer Audit Manager, British Aerospace (Commercial Aircraft) Ltd.

At the risk of spreading disillusionment, adopting the best practice in ideal working conditions does not necessarily guarantee the best results. Often, having those ideal conditions and best practices in place can throw up, at a practical level, a series of difficulties which must be overcome before optimum results are possible. Internal Audit involvement in the systems development life cycle is in no way an exception to this rule.

There is, though, no reason actually to become disillusioned, because any problems encountered are by no means insurmountable. The key is to recognise that they do exist. Before looking at these problems, we will first examine, briefly, the ideal framework in which Computer Auditors should tackle systems developments.

THE IDEAL

The most favourable conditions for Internal Audit would include:

- the adoption of a structured development methodology (such as SSADM) by the IT department;
- a user-led project management team;
- formal approvals to proceed, at key stages of the project, including approval by Internal Audit;
- agreed Internal Audit involvement in the development of controls during the project rather than reliance on post implementation review and criticism of controls at a too late stage;
- an effective Quality Assurance function to monitor the application of IT departmental standards;
- a properly trained and resourced Computer Audit function that has credibility in the eyes of the IT department and user community.

WHERE DO PROBLEMS OCCUR?

As is now generally accepted, the ideal is for Internal Audit to ensure that controls are built into a system from the earliest stage so that expensive system changes are avoided. This approach works well for developments lasting up to about a year - ie. they can be encompassed within a single annual audit plan, or at most overlap two. The approach is also effective for much larger projects if they are broken down into a number of managable units.

However, for strategic reasons, an organisation may embark on a major systems development costing several million pounds and lasting 2-3 years or more - eg. a major distribution system or customer billing system. This is likely to be the highest risk system touched by Internal Audit so it cannot be ignored. Yet it is here where a small department - where Computer Auditors can be counted on the fingers of one hand, as is quite common, will encounter difficulties.

These difficulties will occur in three areas :

- the impact the project will have on the department's plan and resources;
- the extent to which involvement may blur the department's role and priorities; and
- the relationship the department has to adopt with user and IT management.

The solutions to these problems outlined below are based on the experience of a number of system developments and in many cases were learned the hard way.

PLANS & RESOURCES

If the Internal Audit department is small - as many are - it is unlikely that a large team could be assembled to tackle a large scale development project without significant impact on the department's other work. In any case there are unlikely to be many suitably qualified staff, even if other work could be sacrificed. At best the team might number two or three people but at worst the work might be allocated to a single Computer Auditor. In this environment the limited resources available must be managed very carefully.

The first point to note is that the Internal Audit department is not fully in control of its own plans as these will be at the mercy of the project's own progress. And of course as major projects almost invariably overrun, the simplest rule is that inevitably the audit plan will have to be changed.

This is likely to manifest itself in three ways:

- The project size, risk or timescales may have been underestimated in the original plans and, as a result, the audit effort required in the audit plan may require a significant increase.

- Audit work may be scheduled for a particular date which then cannot be performed because project progress is too slow. Perhaps a Statement of Requirements was scheduled for review and comment by a particular date but was delivered late by the project team.

- Conversely at critical times, particularly immediately prior to the go live date, the project may generate more work than can be handled by the project team, necessitating the drafting in of extra auditors (perhaps non-computer auditors) who will not have the same level of knowledge as the project team.

These problems require that the department's annual audit plan be developed with flexibility in mind. All computer projects should be ranked according to risk so that should the major project require extra resource it is clear from the outset where that resource will be taken from. A reserve list of projects should also be drawn up to provide work in the event of the major project's slower than anticipated progress causing a slack period in the department. Needless to say, this approach should be agreed "up front" with management so that they understand the need for such flexibility and their expectations of what will be produced by Computer Audit are realistic.

The second major resource concern is the continuity of staff, since if a project is to last a number of years there is a danger that in that time the department could lose one or more people whose expertise may be irreplaceable. As auditors we may often counsel others about placing undue reliance on key personnel who could easily be lost to the organisation. Involvement in a major system development is an area where we could fall into that trap ourselves.

The insistence on a high standard of working papers is a vital step in ensuring that if a person is lost to the department, all their knowledge will not go with them. That, however, is only part of the solution as many things - in particular the personal contacts and relationships built up over a long lasting involvement in a project - cannot be covered even by the most immaculate working papers.

It is essential therefore that wherever possible a team approach is adopted with different auditors being allocated different responsibilities within the project with audit management giving overall guidance. Exchange of information and ideas must be encouraged within the team so that there is a single pool of knowledge rather than a number of isolated ponds. The team should therefore be resilient to loss of a single member.

However, should there be no other option but to allocate the project to a single individual, then audit management must ensure that it maintains a working knowledge of the project. Almost certainly this will require audit management to have a greater involvement in the project than they might expect.

Also, it should be borne in mind that the auditors working on a major project require motivation and one way of providing this is by ensuring that they are given other assignments to work on during its life. This will help prevent boredom and the feeling that their skills are not being fully utilised or developed. There is, after all, no need to increase the likelihood of losing important expertise.

CLARITY OF ROLE & PRIORITIES

Much of the success of systems development auditing, as with general auditing, is dependent on relationships with auditees. Many people involved in a major project - both users and IT staff - may not have a clear idea of what the computer audit role in the project is about. Many problems will be avoided if an awareness of that role is promoted - via publicity handouts or briefing of the project team - but before even this stage is arrived at, it is necessary for the members of Internal Audit to be aware of their role and priorities.

By this last statement, I do not mean knowing the departmental terms of reference and organisation structure but, really, recognising one's own limitations.

The greatest limitation of all is knowledge. The auditor will be expected to comment on the level of control in the system as a whole whereas other members of the team are drawn from specialist business or IT areas. The auditor must recognise that he cannot have the same level of detailed knowledge as these people and therefore must be careful not to be side-tracked into arguments which are not about high- risk areas of the system. His credibility must be built on making sensible recommendations about control.

Whilst this limitation may be seen as a problem, in reality it can work to the auditor's advantage as it forces him to recognise that he must concentrate on

the high risk/high business impact areas of the system if he is to make an effective contribution. Also he is forced into developing controls in partnership with specialists in the project team drawing on combined knowledge. This moves audit away from being a confrontation and hopefully ensures a much more effective implementation of controls.

Unless the auditor is involved in the project full-time, he will be away from it for perhaps significant periods. Whilst events during these times may not be relevant to the control of the system, he will need to keep in touch with progress - if for no other reason than to plan his next involvement. The loss of such effective communications can severely damage credibility and can at times be an acute problem.

There is no simple recipe for maintaining good communications. A lot will depend on the auditor's own personality. He will also need a keen awareness of who are the key members of the team with the best knowledge, so that he perhaps only needs to make two or three phone calls to gain an up-to-date picture. This may be described as building up a network of "grasses" as the most useful people are, of course, those who give you a picture of how things really are rather than the party line. Basically, ensure you make good contacts and cultivate them.

A key point of contact will be the Quality Assurance function of the IT department as they will occupy a quasi-audit role within the project by monitoring the application of IT standards. It is also essential that the respective roles and responsibilities of QA and Computer Audit are laid down at the outset so that their contribution to the project is optimised. Ideally, QA should be the source of assurance that the project is being adequately managed and controlled enabling Computer Audit to concentrate on controls within the system itself.

However, a word of warning must be given here. Computer Audit should express an opinion on the control over the project and if it wishes to rely on QA then it must be sure that QA's work provide the required assurance. However, QA is a resource of the IT department and can be diverted to a non-QA role should the major project be running behind schedule - the IT department's priority being seen as delivery on time more than compliance to its standards. Should this happen, Computer Audit will need to review its own work plans to cover any gaps left by the loss of QA.

A PARTNERSHIP APPROACH

If the above is successful, a systems development audit is then almost conducted in partnership with the project team. This can then help to overcome one of the major problems of resourcing - a potentially heavy involvement in pre- implementation acceptance testing. If the users have really taken ownership of the controls over the system then there is no reason why Computer Audit should not rely on their testing to verify the controls - after all user testing is meant to be independent testing of the system and the system includes controls. A review of results would then be conducted by Computer Audit before an opinion on the controls is expressed.

There is, of course, a pay off and that is the extent to which Internal Audit may have to compromise on control at implementation. If a project is behind schedule, the users may well have to accept the deferral of certain facilities until after implementation or otherwise compromise an initial implementation date. Internal Audit may be pushed to compromise as well and this is where the partnership approach can be seen as a problem and where many of the benefits can be lost.

The only solution is to be realistic and accept that if Computer Audit does not compromise, significant business benefits could be lost and asking whether the non- implementation of a control out-weighs those benefits. It is really a matter of going back to what we said above - be sure of Internal Audit's priorities. It is these that will determine whether compromise is justified.

IN CONCLUSION

It is accepted that the ideal conditions outlined at the start of this article do not hold good everywhere - some Internal Audit Departments might be glad if projects were subject to a structured development methodology without worrying about what is required to give the go ahead for implementation of a system. Nevertheless, it is worth stating that achieving ideal conditions does bring with it a new set of problems.

The more involved one becomes in systems development auditing, the more clearly it can be seen that the ultimate solution to the problems encountered is by adopting a partnership approach. This in turn requires the auditor to be very clear as to where the line of independence and compromise is to be drawn.

ACKNOWLEDGEMENT: With thanks to Karen Coates of City University for assisting with the preparation of the text for this article.

COMPUTER SECURITY - A STEP TOWARDS TOTAL CONTROL

BRIAN WALLIS

Westminster City Council

The topic of computer security is well documented but the practical solutions are quite complex. There is a need for all users and computer auditors to monitor the current user and business needs on a timely basis.

The list of products on the market is endless, and to review and evaluate your security requirements is a time consuming business and should be approached in a serious way.

All too often the lure of purchasing a product that is well documented and offers a solution to all your needs, actually falls short of providing an effective barrier to unauthorised access to the computer system.

The major areas to be considered when evaluating a particular product should focus not only on the 'front-end' security but should also consider 'message integrity'. This involves installing a facility between components of the computer system, to provide security against manual intervention during the processing of an individual transaction.

The subject of cryptography is quite involved but certainly appears to provide a much safer way of protecting your data.

The main concern for any user has to be the comfort of knowing that any transaction being processed will be subject to validation, and the transaction content is exactly the same at both the sending and receiving end.

The subject is an interesting one and should be explored to the fullest, obtaining a method of securing information between workstations and 'host machines' is essential in order that maximum security can be achieved.

The installation of RACF or ACF2 meets most access control, requirements, and if installed effectively provides the users with a secure entry point to the mainframe computer. However, there is no 'final' solution to the security problem for the business user, but steps taken to identify and install protection beyond the current tried and 'tested' methods should be investigated by all I.T. staff concerned.

The overall view of a safe computer processing environment includes the presence of :

- Access Controls
- Personal Authorisation
- Data Identification
- Data Validation
- Program Integrity
- Output Controls
- Data Protection

AND

SECURITY BY MANAGEMENT; SECURE THE ENVIRONMENT AND YOU WILL CONTROL THE BUSINESS

PEOPLE

BILL BARTON BA FCA CISA

Bill read Economics and American Studies at the University of Keele and then joined Coopers and Lybrand in London. He qualified as a Chartered Accountant with Coopers and whilst there spent two years in the Computer Audit Group. He then worked as an Audit Manager for Price Waterhouse in Brussels for a number of years covering both standard audit and computer audit work. During that time he performed reviews and taught in a number of European countries and became a member of the Belgian Accounting Institute.

He is now Computer Audit Manager for The Rank Organisation Plc and is currently involved with the introduction of Data Security Guidelines into the organisation.

Bill is a member of the CASG Management Committee with responsibility for long term planning.

VIRGINIA BRYANT MSc. FCCA MBCS

Prior to joining City University, Virginia spent twelve years in industry and the accountancy profession gaining experience of audit and computerised accounting information systems.

She started her career with the South Western Electricity Board, then in 1973 she joined Nabarro Nathanson (Solicitors) and took responsibility for designing, implementing and managing computerised systems that provided major support functions such as legal time costing, payroll and pension scheme accounting.

In 1980 she joined H.W.Fisher & Co. (Chartered Accountants), with whom she undertook a range of accounting, audit and investigation work.

Since 1985 she has been at City, as Lecturer in Business Computing, where she specialises in the design of accounting and financial information systems and the financial management of IT. Working in a department which trains about 160 systems analysts each year she has the opportunity to 'indoctrinate' them at an early stage in their careers about the need to build controls into systems and about the role of auditors as experts in control evaluation.

She is also interested in measures for computer systems evaluation and was recently Chairman of the UK Computer Measurement Group's DP Accounting Group.

After a CASG meeting a year ago she responded to a call for helpers to start up a Group journal, and you know the rest.....!

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 responsibility is accepted for the correctness of items. Further details should be sought from the event organisers whose details are given at the end of the list. Listing is free. If you have details of an event that may be of interest to other members please send details to; A.J.Thomas, c/o Rob Melville, Centre for Internal Auditing, City University Business School, Frobisher Crescent, Barbican Centre, London EC2Y 8HB (Copy deadlines are shown on page 10)

TITLE	SPEAKER\LEADER	DATE	LOCATION	ORGANISER
		1991		
Getting the Most out of Your Audit		12 February	London	CAET
Managerial Auditing	Gerald Vinten	11-15 February	London	MDC
Risk Analysis Techniques for Internal Audit Planning	Andrew Chambers	19-20 February	London	MDC
Risk Assessment during System Design (CRAMM)	Stephen Daniels Touche Ross & Co.	21 February	London	EDPAA
Microcomputer Security Guidelines	David Phyall	22 February(pm)	West Bromwich	IIA-Midlands
A Modern Approach to Systems Auditing	Keith Wade	25 Feb-1 Mar	London	MDC
The Impact of Change		27 Feb - 1 March	Blackpool	NCC
Value for Money Auditing		28 February	London	CAET
Audit of Small Companies		1 March	London	CAET
Efficient Personal Computer Operation		4 March	London	CAET
Executive Entry into Internal Auditing	Andrew Chambers	5-7 March	London	MDC
How to Control and Manage the IT Function	Grenville Mills	15 March	London	CHARTAC
Audit of Pension Schemes		7 March	London	CAET
Networking		11 March	London	CAET
Spreadsheet Good Practice	Jonathan Batson	12 March	London	CHARTAC
Internal Auditing (II)		12-14 March	London	CAET
Introduction to Internal Audit	Georges Selim	18-22 March	London	MDC
COMPACS Annual Conference		19-22 March	London	IIA(UK)

TITLE	SPEAKER\LEADER	DATE	LOCATION	ORGANISER
		1991		
Internal Audit Management and Planning		20 March	London	CAET
Auditing Value for Money in IT.	Audit Commission	21 March	London	EDPAA
Effective User Control of Computer Systems		21-22 March	London	CAET
Managing a Multi-National Audit Division	Mike Tyrer British Telecom	22 March (pm)	Birmingham	IIA-Midlands
Seminar for Directors of Internal Audit	Keith Wade	25-26 March	London	MDC
Risk, Materiality and Audit Planning	Mike Thexton	9 April	London	CPE
Risk Management		17 April	Nottingham	CIPFA
AUDIT CONFERENCE		17-19 April	Harrogate	CIPFA
The Law and Computer Security	Gerald Vinten City University	18 April	London	EDPAA
Internal Audit in Banks	Peter L. George	21-26 April	London	MDC
Auditing in an IT Environment (I)		24-26 April	London	CAET
Fraud & Corruption within an Organisation	Michael Levi Cardiff University	26 April (am)	Birmingham	IIA-Midlands
Fraud & the Auditor's Responsibility with regard to PACE	Tony Cavaciuti Gwent Constabulary	26 April (pm)	Birmingham	IIA-Midlands
Challenges for Audit Management		1 May	London	CIPFA
The Audit of Human Resources		2 May	London	CAET
Using the Micro to Enhance Audit		3 May	Coventry	CIPFA
Computer Virus Protection	Grenville Mills	9 May (pm)	London	CHARTAC
Recent Developments	Georges Selim	9-10 May	London	MDC
Managerial Auditing	Gerald Vinten	13-17 May	London	MDC
Creating Confidence in in Information Processing	IFIP SEC'91	15-17 May	Brighton	Elsevier
The Audit of Building Societies		16 May	London	CAET

TITLE	SPEAKER\LEADER	DATE	LOCATION	ORGANISER
		1991		
The Audit of Management Information Systems	Paul Collier Exeter University	17 May (pm)	Birmingham	IIA-Midlands
Introduction to Internal Audit	Georges Selim	20-24 May	London	MDC
IBM CAATT Software	Roy Bradford IBM, Paris	23 May	London	EDPAA
Auditing in an IT Environment (II)		30-31 May	London	CAET
Executive Entry into Internal Auditing	Andrew Chambers	4-6 June	London	MDC
Risk Analysis Techniques for Internal Audit Planning	Andrew Chambers	11-12 June	London	MDC
Personal Coaching in Interviewing Skills for Auditors	Terence Bates Bryan Platt	13-14 June	London	MDC
Internal Audit in Banks	Peter L. George	7-12 July	London	MDC
A Modern Approach to Systems Auditing	Keith Wade	8-12 July	London	MDC
Introduction to Internal Audit	Georges Selim	23-27 September	London	MDC
Executive Entry into Internal Auditing	Andrew Chambers	1-3 October	London	MDC
Personal Coaching in Interviewing Skills for Auditors	Terence Bates Bryan Platt	3-4 October	London	MDC
Risk Analysis Techniques for Internal Audit Planning	Andrew Chambers	16-17 October	London	MDC
A Modern Approach to Systems Auditing	Keith Wade	21-25 October	London	MDC
Managerial Auditing	Gerald Vinten	28 Oct-1 Nov	London	MDC
Seminar for Directors of Internal Audit	Keith Wade	20-21 November	London	MDC
Internal Audit in Banks	Peter L. George	24-29 November	London	MDC
Introduction to Internal Audit	Georges Selim	25-29 November	London	MDC

TITLE	SPEAKER\LEADER	DATE	LOCATION	ORGANISER
		1991		
Risk Analysis Techniques for Internal Audit Planning	Andrew Chambers	4-5 December	London	MDC
Executive Entry into Internal Auditing	Andrew Chambers	10-12 December	London	MDC

Many of the above items 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;

CAET Courses in "Operational Auditing" by the Management Centre Europe (ref. 1296-17), Telephone (Brussels) 32 2 516.19.11 ext 934. Fax 32 2 513.71.08.

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)

CPE Courses run by CPE courses Ltd. Aldine House, Aldine Place, 142 Uxbridge Road, London W12 8AW
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 - Seventh International IFIP Conference organised by IFIP and BCS under sponsorship of Digital Equipment Corporation.
Enquiries to Kay Russell, Elsevier Seminars, 256 Banbury Oxford, OX2 7DH.
Tel: 0865 512242

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. Welton 0242 236111)

IIA(UK) Conference run by the Institute of Internal Auditors (U.K.), 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 EC2Y 8HB
Tel: 071 920 0111 ex. 2278 and 2359 or 071 374 0041 (direct line)

NCC National Computing Centre Information Technology Conference, Sales Administration (Events Bookings) NCC, Oxford Road, Manchester, M1 7ED.
Tel: 061 228 6333.

ABSTRACTS

Read any good 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.

INTERNAL AUDIT

Auditing PCs *A new regular column started in the Internal Auditing Journal in December 1990. This is written/edited by John Silltow. Part of the column includes a "clinic". December 1990 and January 1991's "clinics" cover viruses and are much more useful than the normal theorectical articles one often reads.*
(Reported by Malcolm Lindsey)

SECURITY

Security Videos; *All 20-35 mins long. Supporting booklets also available. Maybe useful for in-house training courses ?*

The Survival Game - Computer Disaster Planning

Dangerous Transactions; *Case study approach demonstrates the need for cooperation between technical and financial staff. Also explains the use of new technology in computer audit work.*

Data Insecurity;*A data security review leads to a number of disturbing discoveries...*

Data Security:the facts; *Assesses the risks from radiation eavedropping to a discarded printer ribbon.*

Computer Risk; *The video looks at the need for a risk survey and the practical problems an organisation can take to minimise the risks*

From: TV Choice, 80 St Martin's Lane, London WC2N 4AA
Tel:071 379 0873

The Threat to Computer Systems - Learning the Rules of Risk
A systematic approach to the analysis of risk can mean the difference between survival and collapse. A qualitative and quantitative assessment can minimise the cost of protection.

CARTER R. -**Accountancy** - May 1987 pp.124-125

The Psychology of Computer Crime - *The huge losses computer criminals inflict on business every year could be much reduced if the victims did not concentrate exclusively on security technology but tried also to understand what really lies behind this all but unique offence.*

CARTER R. -**Accountancy** -April 1988 pp.150-151

ABSTRACTS continued

SECURITY cont.

EFT and the Auditor -*The international financial communitystands to benefit from the control, security and audit lessons a major Australian bank learned when it opted for electronic funds transfer.*

PARKES H. -**Accountancy** -March 1988 pp135-138

Data Integrity and Security of the Corporate Data Base:The Dilemma of End User Computing; *This article addresses the data integrity issues and security risks created by the advent of end user computing. The author proposes possible alternatives which do not inhibit the growth of end user computing, yet provide support to the database administrator's function. Activities such as uploading, downloading, data editing and concurrency control are also discussed in this paper. In addition, microcomputer networking is proposed as one means by which a dtabase administrator may ensure data integrity and security in an end user environment.*

CORMAN L -**ATA BASE** Fall\Winter 1988 pp1-5

Computer Access Control Policy Choices

OLSON I & ABRAMS M -**Computers & Security-** December 1990 pp699-714

GENERAL

Controlling IT Systems; *Andrew Chambers considers the advances and risks that new technology systems are bringing.*

Certified Accountant -Dec 1990 p43-44

Systems Assessment in Acquired Subsidiaries; *If most acquisitions have not brought the expected benefits, it could be because the IT issues that arise or. acquisition have not been tackled.*

COSSEY B. -**Accountancy-** January 1991 pp98-99

Tying it All Together: E-Mail At Boeing Aerospace; *Three years ago, Boeing embarked upon an ambitious project to get all of its e-mail users "talking" to each other. Was it successful?*

CORBIN D. -**Journal of Systems Management-** October 1990 pp11-16

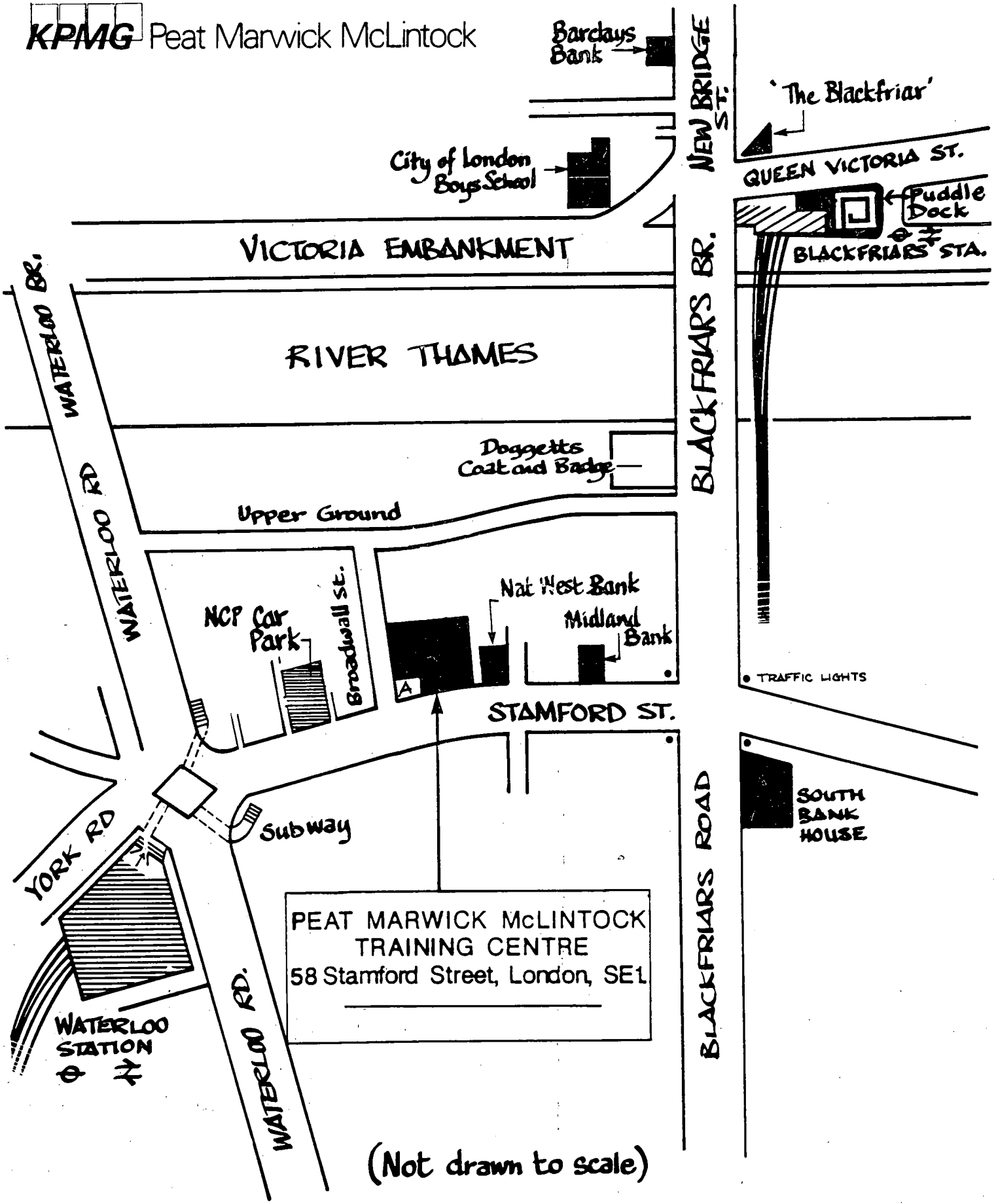
EDI Revolutionizes The Auto Insurance Industry; *An auto insurer and glass replacement specialist link up with EDI and, along the way, transform the way they do business together.*

VEDOCK F. & WHEELESS B. -**Journal of Systems Management-** October 1990 pp17-20

MANAGEMENT COMMITTEE

Chairman	John Mitchell	Little Heath Services	(0707) 54040
Secretary	Ragu Iyer	KPMG Peat Marwick McLintock	(071) 236 8000
Treasurer	Fred Thomas		(0371) 875457
Publications	John Hession	Hertfordshire County Council	(0992) 555323
Members' Meetings	John Bevan		(0992) 582439
Annual Conference	Ian Longbon	CWB Limited	(071) 220 8495
Discussion Groups	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
Editors, Group Journal	Virginia Bryant	City University	(071) 253 4399
	Rob Melville	City University	(071) 920 0111
Long Term Planning	Bill Barton	The Rank Organisation Plc	(071) 706 1111

VENUE FOR MEETINGS



CONTENTS