ISSN 0961-9348

casg
Computer Audit Specialist Group

The British Computer Society

Journal

SUMMER 92

Volume 3, Number 1

Members' Meetings for 1992/93

1992		
October 13th	**EDI security and audit**	Willie List Independent Consultant
October 22nd (full day)	**Discussion Group** **Systems based v. Substantive audit approaches**	Speakers to be announced
November 10th	**TickIT auditing**	Sally James-Owens DNV Quality Assurance Ltd
November 27th (10am-4pm) in Birmingham Contact: Mike Rippin 021 643 8228	**Joint meeting with IIA-UK Midlands District** **Facilities Management**	Speakers to be announced
December 1st	**Outsourcing computer audit**	Mike Shanahan H M Treasury
1993		
January 13th (3.30 for 4pm) venue to be announced	**Joint meeting with IIA-UK Home Counties** **Controlling IT**	Ginny Bryant Rob Melville both from City University
February 9th (2 to 5pm)	**Mainframe to micro security** **– talk with demonstration**	Bob Stuart Computer Associates
February 23rd (full day)	**Discussion Group** **Computer Insecurity**	Topic and speakers to be announced
March 9th venue to be announced	**Joint meeting with EDPAA London chapter** **Annual debate**	Speakers to be announced
April 13th	**UNIX network security**	Greg O'Shea KPMG Management Consulting
May 12th (full day) London International Press Centre	**Annual Conference** **Systems Integrity** **followed by the Annual General Meeting**	Speakers to be announced

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

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

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

SUBSCRIPTION RENEWAL

Yes, it's that time of the year again! Please complete the application form in the Journal and return it with your subscription.

The only exceptions are those of you who joined the Group this year in order to attend the Conference and those few of you who have already paid!

KEEP THAT LABEL!

It would help us if you could attach your current address label to the application form, as it contains your membership number.

Editorial

The Summer issue brings us to the end of another successful season of meetings and discussions. In his Chairman's report, John Mitchell outlines the figures relating to the meetings and the membership. From my position as editor, I have plenty of anecdotal evidence of the continuing growth of computer auditing, and the need for a specialist discussion group. Despite the recession and the personal disaster of redundancy which have affected many of our current and potential members, we seem to be surviving. Considering the very low cost of membership of what is in my mind one of the most erudite and interesting professional bodies around, we give superb value for money in meetings and publications. My end of this is of course the Journal, and I would like to express a very big thank you to all the year's contributors, whose work has kept my eye on the ball in a very stimulating manner. As a lecturer, it is always useful to know what the next big issue is: this year it was operating systems auditing and developing systems. Next year, who knows? My bet is on ISDN, open systems, audit methodologies, and secure systems design. Please contact me if you have any ideas in these areas.

• • •

Talking of secure systems, the Institute of Electrical Engineers (IEE) hosted an excellent seminar on secure systems design, chaired by Willie List. Apart from being superb value, it was among the most useful sessions I have ever attended with speakers on network security, computer fraud, risk analysis, standards and much more. And all for a measly £35 if you were a BCS or CASG member. With all of the competition in computer related conferences these days it is good to see an event that is based on quality and the needs of the profession rather than the needs of the bottom line. Quite a few of your committee were there, and discussions about secure systems continued at the basement seminar room of the 'Coal Hole' in the Strand.

• • •

In this issue we have assembled a formidable range of articles: more on MVS auditing, network security for auditors, disaster recovery, and developing systems. We even have our first response to an article in the journal, from Australia yet! It is good to be able to finish the year on a high note. In the next season, we want to establish a regular training course update, more book reviews and of course keep the standard of article to its current high level. Just think what those of you who have yet to resubscribe are going to miss out on. The journal now has a well deserved break until September

• • •

During the Summer period many postgraduate students from City University and other institutions are looking for placements, work experience or just advice. Generally speaking, they can offer computer audit departments and specialist functions two to three months of usually free assistance while they research for their project dissertations. This year we managed to place several very keen people, who became interested in computer audit during their course. Next year we would like to increase the amount of help we get from the profession. This would also have the advantage of providing potential recruits to the organizations, assuming the recession is over by then! If anyone is interested, please contact Rob Melville, 071 477 8646.

ROB MELVILLE

casg

Management Committee

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

Contents

Chairman's Corner

John Mitchell

Well, the annual conference has come and gone, together with the AGM, and we are now at that pause in our activities where we gather our strength for the next season's excesses. It's not all wine and roses; the programme card has to be prepared for one thing and last minute changes are the norm rather than the exception. Still, I crack the whip a bit and everything seems to sort itself out. It's easy being chairman; you don't actually have to do anything, except perhaps to moan and groan a bit about just how good the *previous* committee was at getting things done!

Another advantage to the job is that people think that you have influence and they invite you along to see new products and the like. Ha, ha, little do they know that us auditors cannot be bought for the price of a beer and a sandwich - champagne and oysters maybe, but not a measly beer. Now where is all this leading to, I hear you ask? Is this definite confirmation that Mitchell has gone of his trolley at last, or simply confirmation that he was never on it to start with?

Well, maybe both, but I do find it amazing how many organisations want us to advertise their products to you, without being willing to provide anything in the way of a discount. In case you have ever wondered what our policy is on circulating third party material to you, it is as follows. Firstly, nothing gets included in our circulation unless we consider it to be of interest to our members (i.e. no junk mail). Secondly, we always ask for a discount. Thirdly, if we cannot get a discount, we charge a commercial mailing rate, or get some reciprocal publicity for our group. Finally, we never release our membership list. By sticking with these policies we consider that our members gain either directly (via a discount), or indirectly (by swelling the funds), from belonging to the group and we salve our conscience when we do decide to include something.

* * * *

The "swap shop" on phantom withdrawals drew some interesting responses and it is certainly a useful way of bringing members together. If you have an area that you would like to gain other peoples' views on, why not ask Rob Melville to include it as a "swap shop" item? On the subject of member participation, Rob was moaning the other day that no one ever writes to the editor. So if you are out there "disgusted of Clapham Common", drop a line to the editor and be the first to be published. He is so desperate for people to write to him that even anonymous letters saying what a great chap the chairman is are likely to be published!

* * * *

Windows 3.1 landed on my desk the other day. Those of you who have bothered to read this column in the past will know that I am a DesqView fan and I feel about Windows in much the same light as the people on the receiving end of the phrase "I'm from internal audit, I'm here to help you". However, I have to keep up with technology, so I keep Windows loaded on my machine (running under DesqView!) to run Windows applications that require Windows to be loaded. It just so happened that as I was reading the installation instructions and had got to the bit about "will applications that used to run under Windows 3.0 run under Windows 3.1 - yes they will, etc., etc.," when my wife handed me a fax listing about thirty packages where this was not the case! Perhaps I'll switch to the new version of OS/2, which is getting good reviews for running both DOS and Windows products better than DOS or Windows!

* * * *

Which brings me to the subject of Open Systems, and I don't mean Unix, which is an awful operating system for commercial applications and is only "open" in regard to operating platform portability. Many more things are becoming "open" via the application of intermediate software. Last week I saw a 386 PC running DOS, Pick and Unix with interchangeability of data and the ability to launch applications in each OS without leaving the one you are currently in. How was this accomplished? By the use of another piece of software sitting on top of them. It was mightily impressive and made me wonder about the control implications of such systems. Especially the problem of where ultimate control actually resided. Was it in within the relevant OS, or was it in the the other package. In this case the user didn't know and didn't care, but then as he told me, he was a data processing professional and, unlike us auditors, was more interested in solutions than problems!

* * * *

As a conclusion, I entered a bookshop in London called the "IT Bookshop" and asked for a book on Pick. "Pick what?", queried the assistant. "The OS", I replied. "Never heard of them", came the reply. "We have books on picking everything, but not on picking OS. Is it Australian by the way?". After more of such confusion, it turned out that the "IT" in the shop's name stood for "Intermediate Technology" and not the "Information Technology" that I had anticipated. They had some very nice books on building windmills!

Have a nice summer. See you next season.

System Development Project Management
Part 2 - Reducing the Risks

Virginia Bryant
School of Informatics, The City University

In Part 1, (CASG Journal Vol.2, No.2, pp16-18), some of the commonly cited reasons for system development project failure were discussed. Failure results from management weaknesses, rather than technical causes. This article will outline how audit involvement can reduce the exposure created by committing resources to a project which may fail to produce the required information system support for the business, within an acceptable timescale and cost.

An audit methodology for the selection of system development controls needs to include consideration of the environmental, planning and methodological support matters outlined. in Part 1. Here the framework of standard system development audit methodology outlined by TRAVIS (8) has been used to illustrate how these matters can be addressed explicitly by including them at the audit planning stage.

The audit planning stage requires the development of an audit focused description of the system development project(s). This will include project familiarization, the identification of the system development components and the critical development threats to those components.

Project Familiarization

In order to agree on useful system development controls, the environment in which system development projects are planned and carried out should be reviewed, and particular attention paid to the existence of policies and procedures for the following;

- The source of the personnel involved in initiating and approving the project should be stated and examined to ensure adequate inter-domain communication and adequate management consensus about the need for, and the outcome of, the project.
- There should be a required minimum level of experience in project management and relevant skills for personnel assigned to project management.
- The project control mechanisms should be established and reviewed for effectiveness. The reliability of project estimation data should be reviewed by management.
- There should be a mechanism to assist in resolving project prioritization disputes.

Project Specific System Development Process Models

The systems development cycle is a recognized sequence of tasks, decision points and supporting documentation, leading to the successful implementation of a system. Within this cycle a common model of the software development process is the 'waterfall' model (Fig. 1).

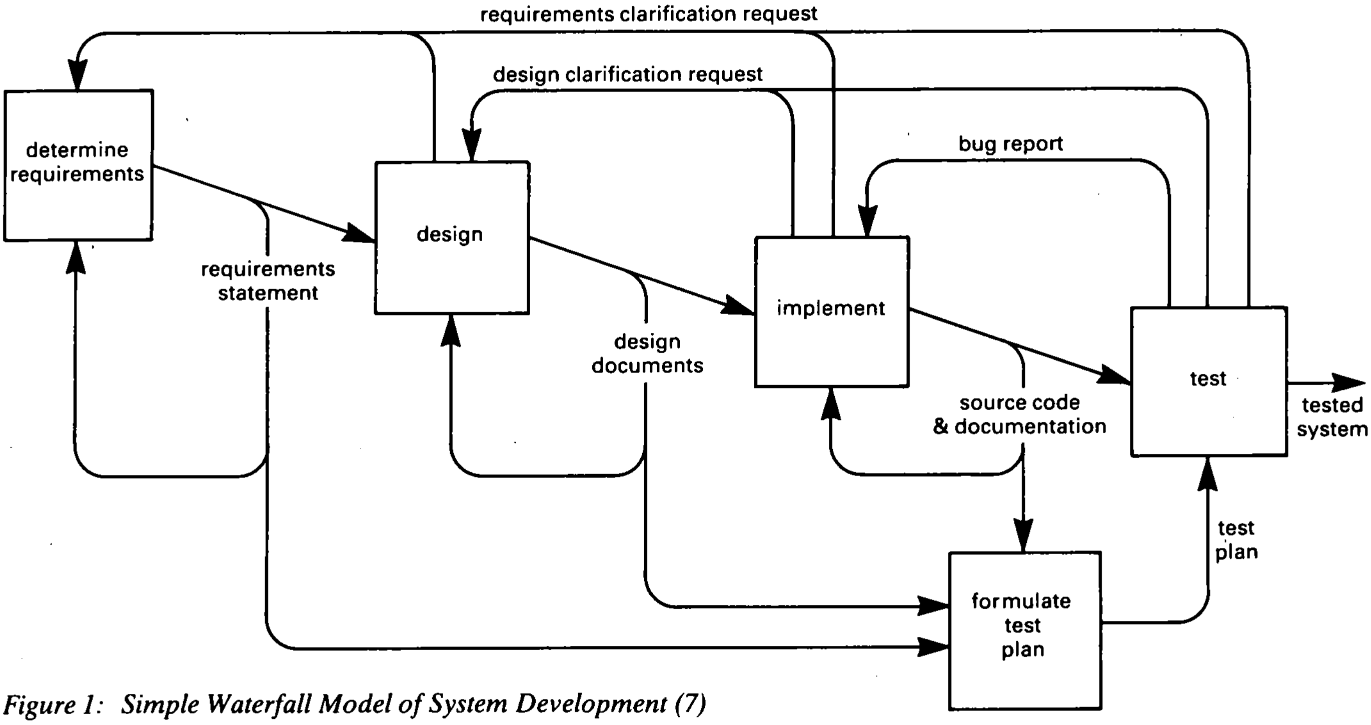


Figure 1: Simple Waterfall Model of System Development (7)

These models are complex and full of ill-defined relationships. Replanning (rather than making *ad hoc* adjustments to existing plans) tends to be undertaken reluctantly, even when it is obvious that things are very different from what was planned. This limits the ability of the model to reflect the system/software development process well, and the lack of process models which aid understanding or support dynamic replanning of projects has been cited as a major limitation in project control (7).

A general purpose model can cater for requirement changes and risk management by incorporating loops back to requirements specification, suitable risk management steps and branches to cope with favourable and unfavourable risk outcomes.

Thus the usefulness of the model used and its utility for dynamic replanning should also be considered.

Identification of System Development Components

When six project managers were asked to identify the major activities or areas to which resources were committed in the projects they managed, the following were most commonly given;

Determining Project Scope
Investigation
Analysis
Design
Development
Testing
Documentation
Installation
User Training
Implementation
Project Management

(The items listed above represent the most frequently occurring ones. An alternative list is given in (8) on page 219. Another approach would be to adopt a standard list representing the stages in system development methodology such as SSADM.)

Identify Development Threats

Anything which could lead to a delay in the timing, an increase in costs or a change in the scope of the project is a threat to the system development process. The implication of the threat will depend on how far the project has proceeded when the threat occurs.

One definition of a threat is "...the absence of one or other of the items .... which form part of the specific project development methodology that is being followed" (8). The project managers questioned had difficulty with this approach and preferred to identify threats, more generally, as 'loss of staff', 'inadequate tools', 'design failures/errors', etc. (5). The effect of these general threats on the system development components need to be assessed.

Using the idea that threats to the success of the project arise from inadequacies in the environment, the specific plan or the methodological support, the adequacy of the following should be reviewed;

ENVIRONMENT
Terms of Reference
Development Standards and Guidelines
Internal Audit
Quality Assurance
Training Provision
Project Steering Committee
Project Management
Data Administration
Project Reporting

PLANNING
Development Plan
Implementation Plan
Time Schedule (inc. Critical Path Analysis)
Resource Scheduling (e.g. Gantt Chart)

METHODOLOGICAL SUPPORT
System Development Methodology
Package Evaluation and Selection Criteria
Process Control Model
Integration of Project Management with System Development Methodology

Construct Development Exposure Matrix

The construction of the development exposure matrix is done by listing the system development components on the vertical axis, and the potential sources of development threats on the horizontal axis (Fig. 2). By estimating the value of the resources likely to be consumed in the development process and the probability of a threatened adverse action actually happening, a figure for the expected value of the exposure can be calculated (analogous to CRAMM).

Select Controls

Once the vulnerable areas have been identified, the next step is to select the most appropriate controls, which should give us a high degree of assurance of the successful outcome of the project, and to agree these controls, in the form of an audit programme with the management in both the user domain and the IT domain responsible for the system development project.

(For a useful ICQ for development controls see (8) pp. 80-90.)

	THREATS	ENVIRONMENT				PLANNING		METHODOLOGICAL SUPPORT						
RESOURCES (System Development Components)	COST	TERMS OF REFERENCE	DEVELOPMENT STANDARDS & GUIDELINES	INTERNAL AUDIT	ETC	DEVELOPMENT PLAN	IMPLEMENTATION PLAN	TIME SCHEDULE	RESOURCE SCHEDULING	SYSTEM DEVELOPMENT METHODOLOGY	PACKAGE EVALUATION & SELECTION CRITERIA	PROCESS CONTROL MODEL	INTEGRATION OF PM WITH SD METHOD	
DETERMINING PROJECT SCOPE		PROB.												
INVESTIGATION														
ANALYSIS														
DESIGN														
DEVELOPMENT														
TESTING														
DOCUMENTATION														
INSTALLATION														
USER TRAINING														
IMPLEMENTATION														
PROJECT MANAGEMENT														

Figure 2 Systems Development Project Exposure Matrix

Once the desirable controls have been identified, the audit programme can be constructed. The testing and evaluation of selected controls, and eventual reporting on controls, can follow.

Can We Learn From Past Mistakes?

Once the system development project is completed, the people involved usually move on to other tasks and rarely get the opportunity to see any overall picture of what happened during the project, compared with what was expected. This limits the opportunity for learning about project management.

The SOMIT survey (1) found that post-implementation reviews were undertaken for all projects by 50% of the respondents, however another study (3) suggested that the main objective in undertaking such reviews is to sign-off the project,passing responsibility for the system from the development team to the users; rather than any analysis of how the project varied from the plan, as a basis for input to other projects.

Moving away from system development projects, it is interesting to note that post-completion audits for capital projects have been adopted by half the major UK companies (6), with the following benefits;

- More realistic forecasting of project costs and revenues
- Increased understanding of what causes project failure
- Mechanism to assist with management assessment
- Improved decision making and corporate performance
- Early identification of potential project failures

System development projects are risky undertakings for most organisations. Audit effort directed towards the management of these projects could reduce the risks, most of which arise from the 'people/management' rather than the 'technical' issues. Consideration of project management under environmental, planning and methodological support should indicate how brittle an organization's project management is. While tools such the exposure matrix outlined here can indicate the best use of audit resources.

Also, although project managers are wiser in hindsight, quantification and modelling of what went wrong is rarely attempted. Post-completion audits would provide useful feedback to the project planning process.

Project management will always be a difficult area because of the uniqueness of each project, but audit support would help project managers to learn from past mistakes.

REFERENCES

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

(2) DE MARCO T. (1988) Software Estimation

(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)

Business Continuity Planning – A Practical Approach

Malcolm Cornish

Malcolm Cornish is a partner in SMH Associates, which provides consultancy services and specialist software for business continuity planning and can be contacted on (0252) 861074.

Internal and external auditors have for years achieved mixed success in convincing management of the need to tackle disaster recovery planning. The increasing move towards distributed processing using PCs, local area networks and minicomputer systems within business units has shifted the goal posts. Business Continuity Planning is the catch phrase of the nineties.

This means that business managers are having to take on responsibility for ensuring the continuity of the business units for which they are responsible. But how can each manager find the time to study up on the issues, identify the information to be gathered and draft complete and coordinated plans which will ensure the survival of the company?

In this article, I identify what I consider to be the minimum information that business units need to gather and suggest a cost effective way to write complete business continuity plans. The article is directed both towards internal auditors, who can advise and cajole business units into action, and business managers themselves who have recognised the need to something but are not that familiar with the issues.

Framework for developing a Continuity Plan

What does continuity mean? In my view, it means being able to provide a minimum level of service to clients, customers and other business partners regardless of any events or incidents that occur. In practical terms, this means continuing to operate effectively during:

- an emergency phase that follows an incident, during which there is likely to be a considerable amount of panic and pandemonium
- a fall back phase when key business activities have to relocate as a result of exceptional circumstances
- a resumption phase during which there is a transition back to a normal business situation.

Because incidents generally affect a physical location, the best approach is to build a continuity plan for a location and all the business units within it. They share common services, are affected by common external factors and have common suppliers, local emergency services and so on. Included at the end of this article is a check list of the key information that a business unit needs to gather.

Having identified the basic information for each critical business activity, consideration needs to be given to potential members of the teams that will manage the relocation and continuity of those business activities. Candidates for the roles of coordinator, stand-in coordinator, team member and stand-in team member need to be identified and the details shown in Figure 1 recorded.

The step that follows is to collate that information into a series of coordinated plans.

Name:	
Department:	
Room number:	
Telephone:	
Home address:	
Home telephone:	
Mobile telephone:	

Figure 1

In addition to business activity details, there is a considerable amount of other information that needs to be gathered. It includes but is not limited to:

- Contact details for all suppliers, external authorities, insurance companies, hotels in the area, local taxi companies etc
- Information about each off-site location including names of persons and relevant contact details, ground plans, route descriptions identifying how to get to the off-site location, officials and members of 'fall-back teams' who will require access.

A more extensive checklist than I can provide here would be useful. I strongly advocate the use of specialist software which can provide either a model plan, as in the case of REXSYS, or a questionnaire, as in the new program Total Continuity System (TCS). Such programs also assist greatly with the collation of the information to be gathered and its future maintenance, without which it would quickly become out-of-date and useless.

Having gathered all the information required, the next step is to produce the Business Continuity Plans which constitute a blueprint for survival.

Writing the Business Continuity Plan

A Business Continuity Plan is a complete set of action plans built around teams. Each action plan must be totally integrated with all other plans if the overall Business Continuity Plan is to achieve its aim. Each business unit plan must include steps for providing all the information, equipment and facilities as well as the key business activities. Other plans must cater for a range of support functions. These include:

- damage assessment
- providing accommodation at fall back facilities
- arranging necessary technical facilities at fall back facilities, including power supply, air conditioning and cabling
- recovering telecommunications and data communications facilities
- making all necessary purchases
- controlling all stocks, including paper and forms required for business activities
- setting up purchasing and expense administration for all fall back teams
- directing and advising personnel who are not members of a fall back team
- arranging office space, supplies and other such requirements
- arranging for the production of documents required
- providing administrative support to all fall back teams
- transporting resources and personnel
- maintaining contact with clients and customers
- keeping all personnel informed of status and progress
- maintaining contact with the media
- monitoring progress
- ensuring that fall back events are recorded by those involved such that a proper evaluation is possible

I would not contemplate starting with a blank sheet of paper or word processor screen. I look to a computer program which incorporates the experience and expertise of those who have done it before in a simple to use package.

My own experience and the results of a recent survey of business continuity planning conducted by the **Survive!** organisation, indicates that most specialist software packages around are too IT orientated and overly complex for the needs of business units. A number of suppliers have responded to this by bringing out simpler versions or completely new packages designed to meet the needs of business managers. **Survive!** is a valuable source of information of specialist business continuity planning packages and can be contacted on (081) 871 2546.

Conclusion

I trust that this article is useful in identifying the information that business units must gather for inclusion in a company-wide Business Continuity Plan. To provide a complete list of everything that needs to go into the complete plan and how to go about it would take considerably longer.

The information required

1 Key business activities that must be carried out:

- on a once off basis, immediately after a major incident;
- on an ongoing basis at an off-site location given there are likely to be severe limitations on space and resources.

2 The type of backup facility required:

- A location which is fully equipped and ready for the business unit to move in and start up the key business activities?
- A location which needs to be prepared after the incident to make it ready for use by the business unit?
- A combination of the two?

3 Key members of staff to carry out these activities. In a disaster situation, the last thing you want are surplus people who get in the way and delay or even jeopardise recovery.

4 Minimum space requirements to accommodate the staff and equipment needed to undertake the key business activities.

5 Requirements for:

- special power supply, gas and water facilities;
- climate control facilities;
- telecommunications facilities;
- data communications facilities.

6 Furniture and fittings needed, including desks and chairs.

7 Special equipment requirements. This should include facsimile machines, photocopiers, microfiche readers, cheque signing and other machines that are vital to carrying on a specific business activity.

8 Computer equipment, including PCs, terminals, printers, modems, mice, bar code readers and any other computer related equipment.

9 Computer software, including PC programs such as WordPerfect,m Lotus, DBase as well as any mainframe applications that are needed to support key business activities.

10 Non electronic data, for example, hard copy computer printout, manuals, contacts, reference books etc.

11 Electronic data including backup copies of data files, information services, such as Reuters, Telerate etc

12 Supplies including special stationery and forms, pencils, pens, diskettes, files etc.

Guidelines for Potential Authors

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

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

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

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

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

Your First MVS Audit

Malcolm Lindsey
EDP Auditor, ARGOS plc

The Spring Journal published a "Route Map" for audit testing on the IBM MVS operating system environment. Some interest was expressed and there are two issues worth mentioning if you are considering using the map as a basis for your first MVS audit.

Firstly, the subject of operator override at IPL time requires further expansion. Secondly, management controls should be reviewed as part of your audit. These issues are discussed below. For good measure I have also thrown in a pictorial presentation of the previously published procedure.

Restricting operator override at IPL time

As well as "OPI" being a specific entry in any IEASYS member, "OPI" can also appear as an optional entry in any individual system parameter. E.g:–

APF = (XX, OPI = No)
The default is OPI = Yes

If such an entry is in IEASYS00 (zero, zero), the value XX will persist even if the operator selects another IEASYS member by using the "SYSP=" option at IPL time.

Therefore if in Step 2 of the "Route Map" OPI = YES, you should try to ensure that as many as possible of the following entries appear in IEASYS00.

APF = (XX, OPI = No)
SCH = (XX, OPI = No)
SMF = (XX, OPI = No)
SVC = (XX, OPI = No)

To add all permutations to the "Route Map" would make it indecipherable. With the above information you should be able to change the map depending upon your OPI settings. To avoid confusion remember that the two diamonds on the pictorial map refer to the **separate** OPI entry in IEASYS00!

Another point is that within each SMFPRMXX member there is an entry of PROMPT or NO PROMPT. The default is PROMPT. Four alternatives are possible.

1. NO PROMPT — means the operator is not prompted for SMF parameters (unless a parameter has a syntax error).
2. PROMPT (IPLR) — prompts the operator to supply a reason for the IPL.
3. PROMPT (LIST) — specifies that the operator can modify the SMF parameters.
4. PROMPT (ALL) — specifies that the operator is prompted for the IPL reason and can modify the SMF parameters.

Clearly options (1) or (2) are the options which should be used in all SMFPRMXX members and the auditor should check that this is so. If Option 1 is chosen a syntax review is advised.

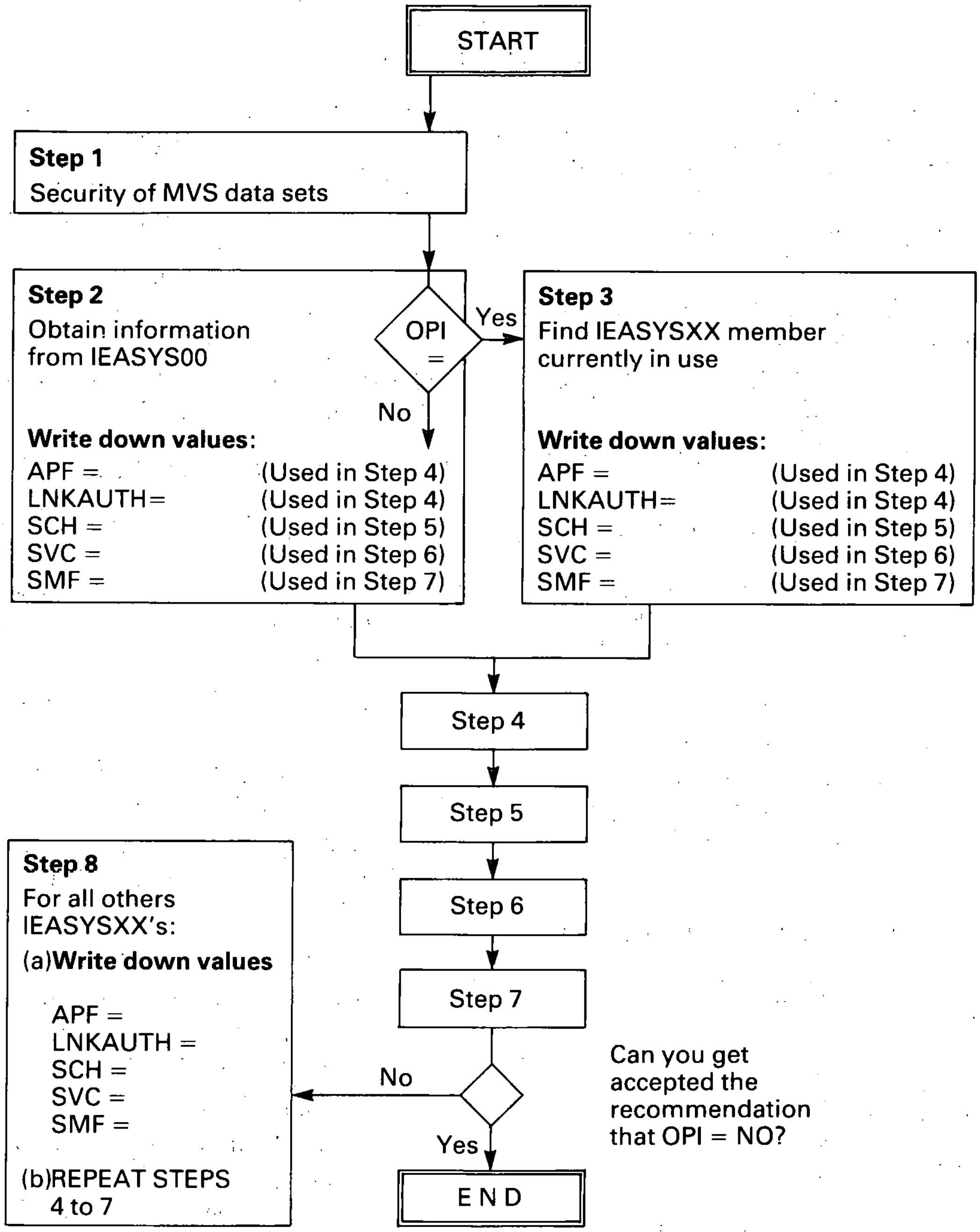
Management Controls to be reviewed

To use the procedure as a basis for your first review my suggestions are:

- Use the "Route Map" to conduct your tests. This should give you a good grounding in the MVS environment.
- Ask what management controls prevent exposures such as
  - unauthorised and uncontrolled change to the SYS1.PARMLIB parameters
  - unauthorised access to MVS software libraries, APF libraries, PPT libraries, SVC libraries and SMF data sets

    Typically you are looking for
    - Standards, for SYS1.PARMLIB settings, etc. Also procedures requiring high level authorisation of changes to standards
    - Operator instructions on IPL
    - Change Control procedures including prior authorisation, management and/or peer review and emergency fix procedures
    - Access control authorisation procedures
- Ask what management controls detect MVS environment exposures.
  You are looking for
  - daily review/sign off of SYSLOG
  - Reports (and procedures for reviewing such reports) of update access to sensitive libraries such as SYS1.PARMLIB
  - Regular review/report of the MVS environment status and review/report of access permissions to sensitive libraries
  - Independent review of all exits
- Gather evidence and conduct tests to satisfy yourself that all management controls are operating satisfactorily.

MVS ROUTE MAP – MARK 1



Conclusion

The main reason I have chosen to tackle the SYS1.PARMLIB entries with the "Route Map" is that it is the only way I have been able to devise a hands-on method of self teaching the relationships, even though you will need to adapt the map to your environment. However, there is also the argument that the tighter the control over operator intervention and the fewer alternative members there are in SYS1.PARMLIB, the easier, cheaper and more effective is the management control. You may well be able to use this argument on the Computer Operations manager, if not the Systems programmer.

You may complete your first audit with some loose ends lying around. Don't despair. This is quite normal. It will also be difficult not to be swamped by technicalities raised by system programmers. Make detailed notes. These, together with further research, will help you plan your second audit.

I hope that the advice given is useful. Provided that in certain areas sample tests are conducted (e.g. APF libraries) it should be possible to conduct a "top-level" review in about 3 to 4 weeks even with little previous experience. This time schedule should be sufficient to include all aspects of the audit including, for example, writing the report.

Contact me if you want further advice or encouragement.

LETTER FROM AUSTRALIA

30 Katrina Street
Turramurra 2074
Australia
13 May 1992

Dear Sir

MVS/XA Route Map

I read with interest Malcolm Lindsey's excellent article but would like to comment on his recommendations in Section 6 regarding User SVCs. As an MVS Systems Programmer of ten years' standing and EDP Auditor of five years' standing (non-concurrent) I feel I can make some criticism here.

User SVC is something of a nisnomer but is IBM's term for all SVCs not part of the operating system. A range of SVC numbers is reserved for operating system use; All others are user SVCs. These include those used by some IBM products, third party software products, and locally written code which we might term *genuine User SVCs*.

User SVCs supplied with IBM and third party software are likely to be installed using SMP/E but there is unlikely to be source code supplied. If there is then a review can be attempted, see below. However in any case the more important controls are change control which should include authentication that software received is as sent by the purported supplier.

In the case of genuine user SVCs source code review is appropriate. The presence of TESTAUTH implies that the writer is security conscious but nothing else. An actual code review by an Assembler programmer (assuming the SVC is written in assemble) is necessary to find out what if anything this macro is achieving. Conversely, the absence of TESTAUTH proves nothing at all. The original and most important function of an SVC is to allow non-supervisor (non-authorised) programs controlled access to supervisor functions.

In fact this is probably the only valid use of genuine user SVCs. This is my final recommendation to the novice reviewing MVS: Any user SVC should have a well-documented justification. A genuine user SVC is halfway to being a code patch in its consequences. It is a maintenance liability and a threat to system integrity. There are valid uses, but a case should be made. Existence of this documentation, and policies ensuring it, is I would suggest of far more significance than the presence of a TESTAUTH macro in the source code.

I hope my comments are of help. They are equally applicable to all MVS systems, whether XA, ESA or vanilla. I would also like to endorse the comment made in Section 4 of the original article regarding the doubtful value of checking for absent APF libraries. I think I can guess the original source of this suggestion, but it has been repeated out of context and has now become a case of the emperor's new clothes.

Missing APF libraries might be a valid thing to check if resources were no object, but it is belt and braces. Tests of the security profiles or access rules are both essential and adequate, as Malcolm Lindsey quite correctly states, perhaps for the first time in print.

Yours Sincerely

Andrew Alder

CASG JOURNAL
SUBMISSION DEADLINES

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

Network Security and the Auditor

Craig Arnall of KPMG Management Consulting highlights the need for network security with increasing use of external communications systems.

IT Security is usually associated with the controls that protect systems against malicious threats, although it is really a much broader topic. As with other aspects of IT, security ought to be tackled strategically rather than with a series of disconnected actions. A properly thought out corporate IT security policy addresses the general concern of ensuring that users can rely on their systems. In the past it has been easier to rely on physical security, based on limiting peoples' access to hardware, sensitive applications and data. With the massive growth in communications networks this has become harder, particularly for organisations introducing links with external organisations over public data services, possibly in different countries.

Security must be approached comprehensively, through analysis and development of an IT security policy. Piecemeal efforts are unlikely to succeed in protecting against the greatest vulnerabilities. In particular, network security cannot be considered in isolation. It must be addressed in the right context: starting at the highest level, through considering overall system security. This will provide the background to analysis of information security which will, in turn, provide a basis within which network and access level issues can be considered.

A security policy sets out how your company deals with threats to the confidentiality, integrity and availability of IT systems. It must consider not only deliberate attempts to break into systems but also address such risks as network failure, faulty circuits, fire and flood. A hardware error introducing spurious bits into a data packet may be just as great a threat as a hacker changing data.

The first step in developing a network security analysis is to document the current situation so as to produce a framework within which decisions can be made. Part of the process consists of identifying the important vulnerabilities. Different people usually have different priorities, so an objective scoring scheme is essential. It helps highlight the areas in which a security breach will cause the greatest impact on the business and hence need to be allowed for.

After identifying the areas of highest impact, the next stage is to analyse them in terms of risk, including consideration of the existing controls against them. One of the most widely used means of assessing the strengths of security controls is given in the US Department of Defense "Trusted Computer Systems Evaluation Criteria", known as the Orange Book (due to the colour of its cover).

That classification provides a progression, starting with insecure systems, then systems in which the owners of applications may specify restrictions on access, then systems in which controls are built in as mandatory features. The most secure category goes even further by requiring that software, including the operating system, is formally proven to meet its specifications.

Initially those categories were only applied to standalone systems because networks could not be trusted. In 1989 though, the DoD produced its Trusted Network Interpretation which allows networks to be classified by the Orange Book evaluation criteria - although recognising that such evaluation is very much harder with networks.

The final stage of a network security analysis is to compare the prioritised risks with the value of the assets at risk. A structured approach is directed towards producing directly comparable scores for each. It gives a rational basis for action, tackling the areas where security is weakest and a breach will cause the most damage. It also provides the framework within which the organisation will periodically revisit its security requirements to verify that they are still being addressed by the controls in place.

Extremely sophisticated protection techniques can be provided in software and hardware but they are utterly pointless without adequate physical security. Software controls that limit access to information cannot, in themselves, counter the threat of an intruder walking out of the computer room with yesterday's backup tapes. In its extreme, physical security might involve isolating equipment in a guarded room, protecting against electromagnetic radiation and only permitting access by vetted personnel.

Here, of course, is the dilemma. A policy of isolating individual systems is at odds with the trend towards networking. As soon as external communication links are introduced, systems can no longer rely on physical access controls alone.

However, if an organisation needs to introduce external communications links then the most straightforward protection is provided by building on the basic principles of physical security. The idea is to lock out anyone without the authority to access systems. Such controls are usually introduced in at least two ways, in networking/transport mechanisms and in application software. These correspond to the lower and upper parts of the OSI seven-layer model respectively.

Access control can be provided at a base level through the use of secure modems and network gateways. Modern modems, commonly used for dial-up access over the telephone network, contain a wealth of relevant features. Individual modems can be programmed with their own passwords, which must be exchanged before any two will communicate with one another. After establishing an initial link users can be required to enter their name, which is checked - maybe locking out those who are only allowed to access systems at particular times of the day. Finally, these systems hang up the telephone and then dial back to the user's known telephone number.

Similar techniques are used for host to host links over a public X.25 data network. The simplest control is to bar all incoming calls to a sensitive system, so that it is responsible for initiating any links with other hosts. Where incoming calls are needed, X.25 permits closed user groups. This ensures that communication is only allowed with trusted systems, which can be further verified through an exchange of passwords. Further protection can be provided through traffic encryption.

It is therefore reasonably straightforward to set up security controls that limit access to known systems. In most cases these will be just as effective as having a security guard checking identity cards at the front door. Remember, in the same way that an ID card can be forged, the determined intruder may still be able to get around such controls.

Network security is a particular concern for those organisations introducing open systems. Open communications doesn't mean insecure communications. It means that networks are more adaptable. Standards provide the technical means of connecting systems but they must also provide the controls to ensure that data, applications and network resources are safe. It is apparent that for many organisations the network is becoming fundamental to the way they do business. They are moving away from centralised mainframes, towards distributed networks of local processors. This trend to downsizing moves computing closer to the workplace but causes greater potential problems for those concerned about security.

One problem is that many businesses are trying to encourage communication rather than restrict it. Some may provide information services to potential customers. Others wish to use electronic trading like EDI or EFT/POS. Those relationships are based on contractual arrangements between people and organisations, not the network addresses of their computers.

There is no such thing as absolute physical security, so it is necessary to rely on other controls. Software checks are built into networked applications and, equally importantly, in the working environment. Passwords are currently the most common means of authentication. After establishing a user's identity, software can use a database of access rights when attempts are made to use resources. Typically, data can be protected at either the file, record and field level. Application services and entire systems can be protected, although all such measures rely on trusting the user authentication mechanism. Greater assurance can be provided with 'smartcards' and progress is being made with voice, fingerprint and retina recognition.

As distributed systems become more commonplace there will be an increasing need for general purpose security services for use by applications. Progress is being made in the international standards community, initially driven by the commercial imperative for security in messaging (X.400), directory services (X.500) and financial systems. The most promising developments use public key encryption and digital signatures. Public key encryption provides one (published) key which scrambles data addressed to a company and another (secret) key, with which the company decodes it. Digital signatures use encryption to provide an assured means of verifying and authenticating the originator and contents of transferred information. They can be used in a public network environment, provided there is a means of establishing trust between systems. This trust can be brokered by secure 'Certification Authorities' that will verify initial contacts between organisations.

Although protective technology is becoming much more reliable than in the past, it is now even more important to get the balance right between the controls provided by automatic methods and those by manual procedures - both to prevent security breaches and to limit the damage when they do occur. It is therefore essential to put in place both organisational and procedural controls. Although technology based controls can provide a high degree of assurance, technology changes rapidly, as do systems. There is no substitute for regular reviews in the form of an IT security audit to be confident that the business is secure.

Chairman's Annual Report - 1991/92

This is the text of a report given by the chairman at the AGM

Introduction

Four years have now passed since I first had the honour to address you as chairman of this group. During that time, the foundations laid by my predecessors have been consolidated and expanded by the hard work of your management committee. Unlike many other professional groups, ours is on a firm financial footing and this report is really a tribute to the members of the committee who have made this possible.

Management Committee

Your management committee comprises four elected positions (chairman, secretary, treasurer and auditor), as required by the rules of the BCS, and a number of co-opted volunteers. The chairman is required to be a BCS member and it is desirable that the other elected officials, with the exception of the auditor, are also members, although there is some flexibility on this point.

There were several changes to the committee membership during the year, due to changes in members' personal circumstances and a number of members have indicated that they will be unable to serve next season. In all, four committee members have had to relinguish their responsibilities: Harry Branchdale, John Hession, Peter Martin and John Pringle. I an sure that you will join me in my thanks to them and wish then every success for the future.

The list below shows the committee for next season. As you notice, 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 Retired Consultant
Hon. Auditor	Tony Locke Day Smith & Hunter

Members & Associated Responsibilities

Meetings	John Bevan Audit & Computer Security Services
Meetings	Alison Webb Alison Webb Associates
Press & PR	Jarlath Bracken Zurich Insurance
Membership	Jacqui Race National Westminster Bank
Journal	Rob Melville City University Business School
Discussion Group	Steve Pooley British Petroleum
Discussion Group	Chris Birt Independent Consultant
Conference	Ian Longbon CWB Ltd
Conference	Paul Howitt Tesco Stores Ltd
Planning	Bill Barton The Rank Group
Publications	Jacqui Race National Westminster Bank

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. However, in view of our surplus, we have decided not to increase our membership subscriptions this year.

Membership

Our membership records, which have been ably maintained by Peter Martin and his computer tells us that we currently have almost 400 members; a pleasing near doubling of our membership in the last four years. An analysis of the membership shows:

By type of Membership	1992	1991	1990	1989	1988
Corporate	224	245	195	140	139
Individual BCS	63	57	45	33	35
Individual Non BCS	106	78	61	34	37
	393	390	301	207	211

By Discipline	1992	1991	1990	1989	1988
External Audit	42	48	47	41	38
Internal Audit	309	290	214	130	151
Other	42	52	40	36	22
	393	390	301	207	211

The increase in numbers over last year is pleasing, but we still have some way to go in order to reach my own personal goal of 500. We are in the process of producing some new publicity material which highlights the advantages of Group membership and which we hope will push membership towards the 500 level.

Discussion Groups

Two Discussion Group meetings were held during the year; the first dealing with Audit Automation and the second with the Legal Aspects of Computing. Steve Pooley and Chris Birt were responsible for the exemplary administration in both cases.

The format is to have four sessions, each of which is addressed by a speaker for about 30 minutes, followed by about an hours discussion. We limit attendance to a maximum of 30 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.

Meeting Venue

Our new regular venue, at the Institute of Public Health and Hygiene in Portland Place, has served us well and we will be continuing our use of these facilities for the next season.

Member Meetings

The annual meeting programme was ably handled by John Bevan and Alison Webb. The subjects covered, including our annual conference and two discussion groups, were as follows:

1991	Subject	No of Attendees
27th September	Risk Based Audit Planning (joint with IIA Midlands)	46
21st October	Auditing the MVS Operating System	21
30th October	Audit Automation (Discussion Group)	35
12th November	File Interrogation Techniques	17
10th December	Unix Security	33
1992		
15th January	The Impact of SSADM (Joint Meeting with IIA)	65
11th February	AS/400 Access Control	25
25th February	Legal Aspects of Computer Auditing (Discussion Group)	31
10th March	Facilities Management (Half Day Meeting)	10
14th April	Computer Audit in Insurance	12
13th May	Disaster Recovery (Annual Conference)	53

On average, the attendance at our meetings is slightly down on last year, which is disappointing in view of the effort and cost involved in running them. Attendance at the half-day meeting on Facilities Management was especially disappointing in view of its current high profile and the excellence of the speakers.

The Journal

Under Rob Melville's stewardship, our main communication arm with our membership has now standardised on a format which has become the envy of other Specialist Groups within the BCS. For those members unable to attend our meetings it provides valuable information at both a practical and theoretical level on computer audit and control matters.

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

Annual Conference

Our most recent conference, held in May of this year, was superbly organised by Ian Longbon and was on the subject of Disaster Recovery. A very topical area at at the moment in view of the recent terrorist activity in the metropolitan centres.

Liaison with the BCS

During the year the BCS suffered a cash crisis which for some time looked serious enough to financially affect the Specialist Groups. Happily, this has now been resolved, although there are still several outstanding matters that need settling before we will be totally at ease in our relationship with our parent body.

Four members of the Management Committee (John Bevan, Rob Melville, Alison Webb and myself) were invited to submit articles for a special edition of the BCS's *Computer Audit Bulletin* on the subject of Computer Audit. This publication has a circulation of some 35,000 copies and a number of requests for further information on the Group were received as a result.

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 40 members attending to hear presentations on the subject of The Impact of SSADM.

Our first joint meeting with the Midlands Chapter of the IIA in Birmingham was a success, although very few of our own members actually turned up. Perhaps this indicates that there is no great demand for meetings outside of the London Area. However, we intend repeating the exercise next year to establish whether, or not, it is worth holding as a regular event.

We still enjoy good relations with our "sister" organisation, the EDPAA, and we work closely together to avoid duplication of subjects. We have planned a joint meeting for next season which is likely to be in the form of a debate and we may well identify one meeting from each other's programme which can be attended by members of the other group on a reciprocal basis.

During the year, members of your committee also addressed the EDPPA's European Conference and various BCS promotional meetings. This formed part of our policy to take every opportunity to increase the visibility of the Group.

Conclusion

The past year has been a year of great progress which has only been achieved due to the hard work of your management 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
13th May 1992

PROFILES

Jacqui Race

Jacqui studied a Business and Finance Management HND and then joined Rochford District Countil as a trainee accountant in 1984. She spent three years working within the various sections of the Finance Department, to supplement her AAT and CIPFA studying.

After leaving Rochford in 1987 she joined Basildon District Council, Internal Audit Section. She held the post of Principal Auditor and was given responsibility for setting up a computer audit section within the authority as well as supervising the work of the Contracts Auditor.

Jacqui and her team were responsible for all aspects of the authority's computer audit. This included installation, application and system development reviews. She was also responsible for the development and training in the use of CAATS within the audit section.

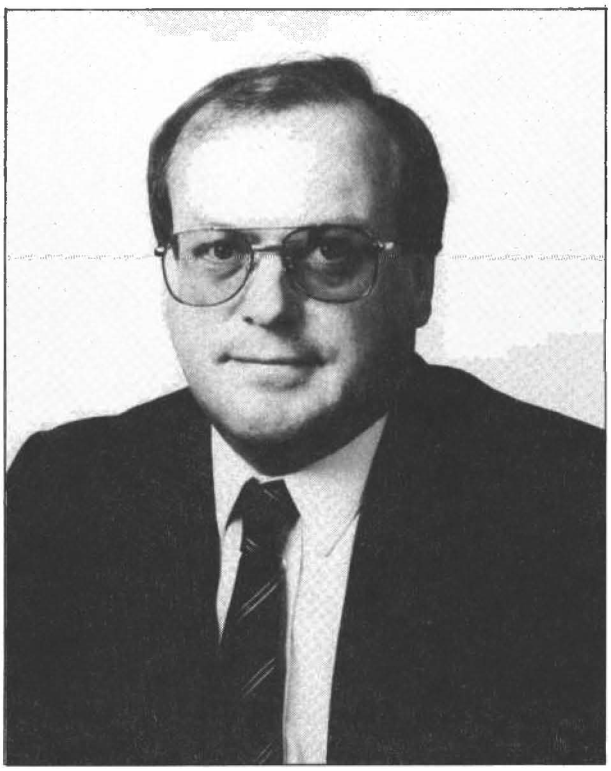
Between 1989 and 1991 Jacqui served as Secretary on the Essex Audit Group, Computer Specialist Group, when she left Local Government to join the private sector. Whilst with the Group, Jacqui was responsible for organising several specialised computer audit courses for public sector computer auditors.

Jacqui is now working for the Information Systems Audit Department of National Westminster Bank PLC, as member of the Applications Audit team. She has spent the past year conducting reviews of high risk financial payment systems, including CHAPS and SWIFT.

For the past two years Jacqui has been studying for her MIIA and QiCA qualifications, and has recently sat her final examinations.

In her spare time Jacqui's main hobby is horse riding.

Jacqui is responsible for the Publications and Membership of the CASG. For any details of CASG publications or membership enquiries, she may be contacted on 071 860 4087.



Paul Howitt

Paul has over twenty years' computing experience and has worked in the manufacturing, distribution and retail industries before he joined Tesco Stores in 1982 as a Senior Analyst Programmer to work on the introduction of scanning and other computerised store systems.

Over the last few years he has been involved in the development, installation and support of several distribution and replenishment initiatives designed to reduce lead times and stock holding in stores and depots.

He became a Computer Auditor in 1989 performing integrity audits, development audits and investigation work. Assistance in the training or raising the computer awareness of non 'computer specialist' colleagues also forms part of his responsibilities.

Paul will be working with Ian Longbon in the organisation of the annual conference.

THE SWAP SHOP

PROBLEMS AIRED PROBLEMS AIRED PROBLEMS AIRED PROBLEMS AIRED

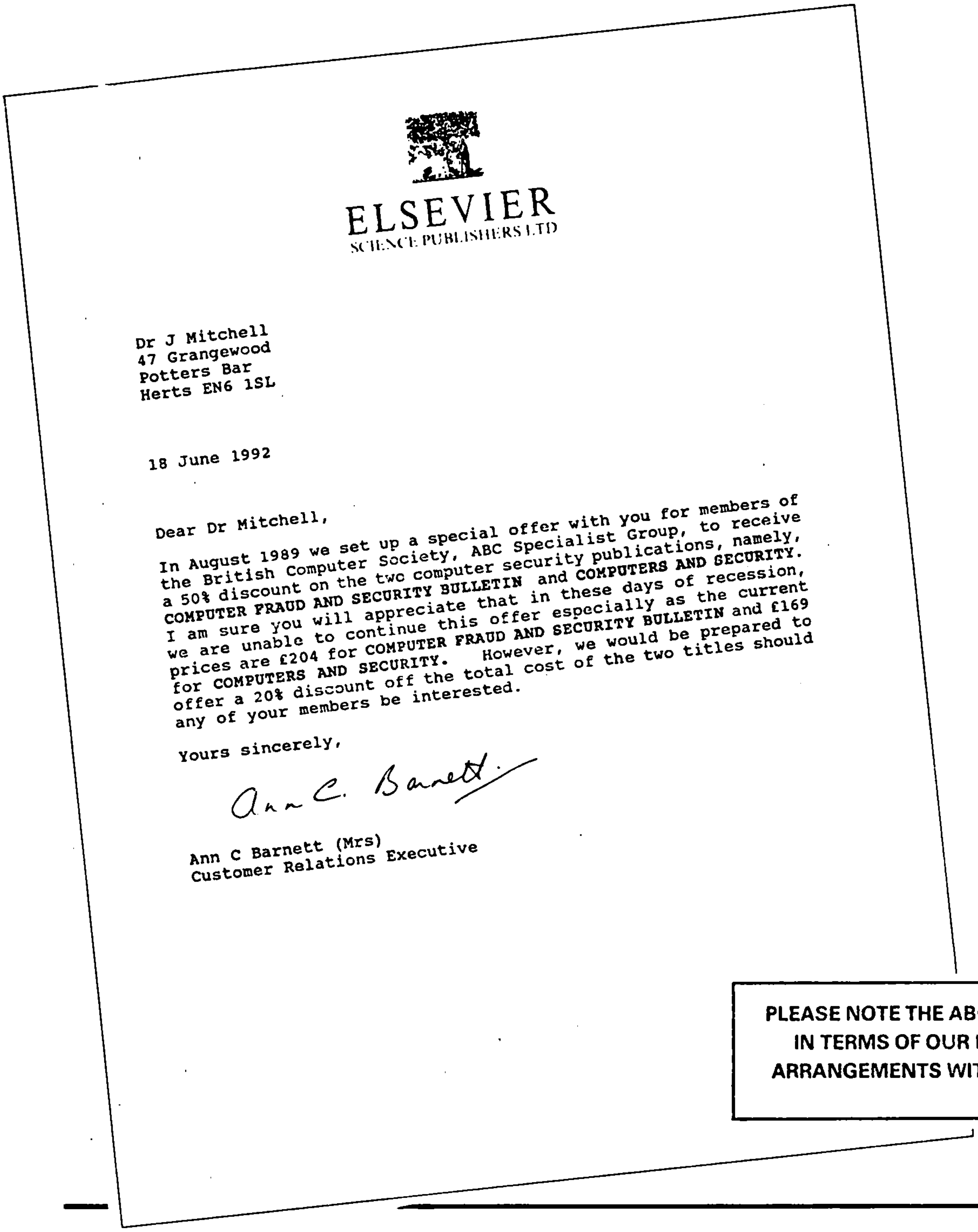
HELP WANTED HELP WANTED HELP WANTED HELP WANTED HELP WANTED

BSI PRODUCT APPROVAL SCHEME FOR SOFTWARE

Kevin Cogman was good enough to draw our attention to a draft document, issued by the BSI, dealing with product approval for accountancy software. If you would like to see what the BSI are up to and perhaps have some input, then contact the BSI at the address below specifying "Document P018V017 Version 1.7, 1992 - Product Approval Sectional Specification".

Mr N B Martin
BSI Quality Assurance
IT & Software Engineering
PO Box 375
Milton Keynes
MK14 6LL

Our thanks to Kevin for drawing our attention to it. If anyone else is aware of similar developments please let the editor know of them so that we can keep everyone informed.



ELSEVIER
SCIENCE PUBLISHERS LTD

Dr J Mitchell
47 Grangewood
Potters Bar
Herts EN6 1SL

18 June 1992

Dear Dr Mitchell,

In August 1989 we set up a special offer with you for members of the British Computer Society, ABC Specialist Group, to receive a 50% discount on the two computer security publications, namely, **COMPUTER FRAUD AND SECURITY BULLETIN** and **COMPUTERS AND SECURITY**. I am sure you will appreciate that in these days of recession, we are unable to continue this offer especially as the current prices are £204 for **COMPUTER FRAUD AND SECURITY BULLETIN** and £169 for **COMPUTERS AND SECURITY**. However, we would be prepared to offer a 20% discount off the total cost of the two titles should any of your members be interested.

Yours sincerely,

Ann C. Barnett

Ann C Barnett (Mrs)
Customer Relations Executive

PLEASE NOTE THE ABOVE CHANGE IN TERMS OF OUR DISCOUNT ARRANGEMENTS WITH ELSEVIER.

Product News

Touche Ross are in the process of releasing an "Intelligent Audit Trail Analysis" product which uses expert system technology to take the drudgery out of analysing system journals and the like. Contact Gary Hardy on 071 936 3000 for more information.

☆ ☆ ☆ ☆

OSPL have announced a new PC security product which monitors program and file usage as well as a host of other things. Contact Richard Downes on 0252 812112 for details.

☆ ☆ ☆ ☆

The IIA-UK have announced the creation of a specialist audit discussion group dealing with STRATUS. If you are a STRATUS user and want to meet other auditors involved in the same area, then contact Ed Hutt on 0532 313000 x3644 for more details.

★ ★ ★ ★

PLEASE MENTION THE JOURNAL WHEN CONTACTING ORGANISATIONS

casg
Computer Audit
Specialist Group

The British Computer Society

Membership Application

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

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

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

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

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

SIGNATURE: DATE:

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

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

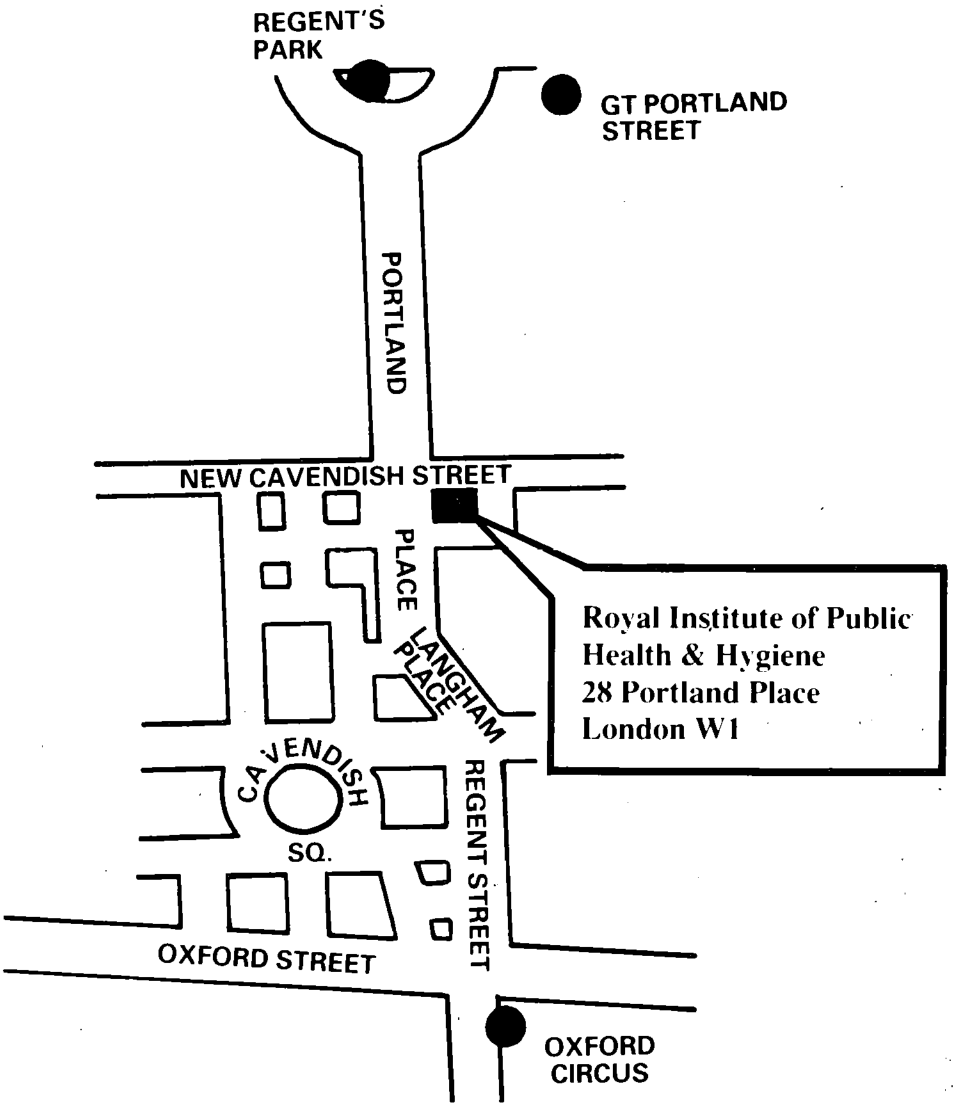
ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

Venue for Members' Meetings


REGENT'S PARK
GT PORTLAND STREET
PORTLAND
NEW CAVENDISH STREET
PLACE
LANGHAM PLACE
Royal Institute of Public Health & Hygiene
28 Portland Place
London W1
CAVENDISH SQ.
REGENT STREET
OXFORD STREET
OXFORD CIRCUS