ISSN 0961-9348

casg Computer Audit Specialist Group

The British Computer Society

Journal

WINTER 1991

Volume 2, Number 3

Members' Meetings for 1991/92

15 Jan 1992	3.30pm for 4.00pm	**CONTROLLING SYSTEMS DEVELOPMENT USING STRUCTURED METHODOLOGIES (Joint Meeting with I.I.A. Home Counties District Society)**		Coopers Lybrand Deloitte 128 Victoria Street London EC4P 4JX
11 Feb 1992	3.30pm for 4.00pm	**IBM AS400 SECURITY**	A. Henderson *Ernst & Young*	Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
25 Feb 1992	9.00am (full day)	Discussion Group **LEGAL ASPECTS OF THE VARIOUS STATUTES OF INTEREST TO COMPUTER AUDITORS**		Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
10 Mar 1992	1.30pm for 2.00pm	**FACILITIES MANAGEMENT**	D. King D. Earle A. White	Royal Institute of Public Health and Hygiene 28 Portland Place, London W1
14 Apr 1992	4.00pm for 4.30pm	**COMPUTER AUDIT IN INSURANCE**	Christine Osman *National Provident Institution*	Royal Institute of Health and Hygiene 28 Portland Place, London W1
14 May 1992	9.00am	**ANNUAL CONFERENCE** **Disaster Recovery**		London International Press Centre
	4.30pm	**Annual General Meeting** **(Admission free to members)**		

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

Editorial

It will not have escaped the sharp eyes of our members that two issues of the Journal have been delivered this time. In true audit style, there may be some who will question the accuracy of the date of the other copy received (Summer/Autumn?). Anyway, rather than relive the nightmares of producing the Summer/Autumn issue all over again, suffice to say that due to an exceptional series of circumstances, production was extremely delayed. For this the editorial team apologises to the membership.

For all the lateness of its publication, the Summer/Autumn issue has been extremely well received by those fortunate enough to have received a copy (we managed to distribute a few at a meeting). Malcolm Lindsey's paper on auditing AS 400 has inspired at least three other auditors to attempt this task. We hope there is more to come of this quality, not just from Malcolm, but other members as well.

In this issue, we have put together some very useful articles: subjects include certification, security and MVS reviews. You will notice that some usual items are not included, in particular the courses guide. This is because getting the information together was a very time consuming task and Fred Thomas is not going to be able to continue combining it with his secretarial duties. It may be that we can start this next year, but it obviously depends on the organizations in question informing us of their programmes.

Some new developments for next year: refereed articles, publication of monographs of the best papers and more regular reviews of books and texts relevant to our profession. This will raise the profile of the Journal, the membership and the Group. Given the specialist nature of our professional activities, and the skills and expertise available within our readership, we should be able to produce some very creditable material.

The issue also has some changes on the editorial side. Ginny Bryant has recently taken on yet more responsibility at City University, which leaves her no time for editorial duties. Many grateful thanks are due to Ginny, who not only managed to get this journal started (an achievement in itself), but also improved the quality of presentation and content to a very high degree. Over the last year she has also been busy grooming her replacement as editor; she will be a very hard act to follow, but it is hoped that professional calm, enthusiasm, sound knowledge and sheer friendliness are all contagious.

We also decided that to take full advantage of the progress of the journal so far, the production side of editorial duties should be passed on to specialists. This issue will be the first to be professionally typeset, and will allow our editorial panel to concentrate on the 'thinking tasks'.

Finally, the compliments of the season to all our readers. As an auditor, who likes to balance optimism with prudence, I leave you to decide whether I mean Christmas, New Year, or Easter . . . .

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		0371 875457
PUBLICATIONS	Jacqui Race	National Westminster Bank	071 860 4087
MONTHLY MEETINGS	John Bevan	Audit and Computer Security Services	0992 582439
	Alison Webb	Independent Consultant	0223 461316
JOINT CONFERENCE ORGANISERS	Ian Longbon John Pringle	CWB Limited Department of Energy	071 220 8495 071 273 0730
DISCUSSION GROUPS	Chris Birt Steve Pooley	Ernst & Young Independent Consultant	071 928 2000 0580 891036
MARKETING & PR	Harry Branchdale	British American Tobacco	071 222 1222
MEMBERSHIP SECRETARY	Peter Martin	E D & F Man Ltd	071 626 8788
PLANNING	Bill Barton	The Rank Organisation Plc	071 706 1111
JOURNAL EDITOR	Rob Melville	City University	071 920 0111 Ext 2342

Contents

Members' Meetings 1991/92		Cover
Editorial		1
Chairman's Corner	John Mitchell	2
TickIT: Certifying Quality Management in IT	Alison Webb	4
Computer Security	Jim Kenney	6
An Introduction to Auditing MVS	Alan Oliphant	11
Annual Conference – Advance Notice		12
Annual Conference – Priority Booking		13
Annual Conference – Programme		14
Membership Application		15
Management Committee		IBC
Venue for Monthly Meetings		Back cover

Chairman's Corner

John Mitchell

In my very first column I pointed out that one of the advantages of being chairman (I refuse to be called a chair) was being able to use this column to sound-off about issues that affected me personally. In the last issue I mentioned how impressed I had been with the service provided by the suppliers of XTREE and how badly Digital Research had performed in comparison when I had experienced problems with its DR DOS 5.0 operating system.

Well, Digital recently released DR DOS 6.0 and so I checked with their technical support people that this would work on my Tandon machine with the funny exchangeable disk drives. Yes it would, I was assured, so I forked out the readies for the upgrade. Would it install? Heck, no. So I then tried installing it on my portable, where I had previously managed to install version 5.0 without any problems. Would version 6.0 load? Nope. So I fired off another software report form (why do they only supply one with the package!) to Digital explaining the problem and asking for a solution.

After a couple of weeks I received an enigmatic response to the portable problem. "Please check the attributes of your COMMAND.COM file", they suggested, but they didn't tell me what they should be! So I checked them out, looking carefully for any read-only settings, etc., but everything looked fine. So I burn the 'phone lines a little more and they ask me for an attributes listing, which I duly send then, along with the contents of my AUTOEXEC.BAT and CONFIG.SYS files for luck.

A week goes by and I receive a telephone call. Now this is real progress, my very first telephone call from them! "You have a memory problem", I am informed. "Yes, well I know the little grey cells are ageing a bit, but ...... "No, no, it's your machine that's the problem". It appears that a measly 512K isn't big enough to cope with the new installation program and some 640K machines are affected too! What's the point I think to myself of Digital promoting an OS which makes more memory available to applications if the installation program itself is so big that it can't run on a 512K box? Still, they did have a work-round which involved me installing it manually, but that was very straight forward, and I now have DR DOS 6.0 running on my portable.

I then used their SUPERSTORE disk compression software on the 20 Megabyte hard disk, which only had 3 megs spare. Low and behold, after 30 minutes crunching I suddenly had 15 megs spare and all my exiting software seems to work fine! Now to my way of thinking it's worth running DR DOS 6.0 on small capacity machines simply for the SUPERSTORE facility. Still no luck with my Tandon however, although I have made a little progress. More in the next issue perhaps?

At just about the same time I also received upgrades to Supercalc 5 and PCTOOLS. The Supercalc upgrade presented no problems at all, well done Computer Associates, but PCTOOLS was a different story. Centre Point software, the PCTOOLS people, had received lots of stick (no, not from me) about problems with their last version and had rushed out an upgrade to solve the problems.

I duly installed it and then went on to run their COMPRESS utility which, unlike the DR DOS 6.0 facility, simply re-organises the disk, but is still very useful in freeing up space and I use it about once a week on my 40 megabyte exchangeable hard drives. This time however, instead of trying to compress my hard disk as I had requested, it promptly tried to do the business on one of my floppy drives instead. No matter what I tried the result was the same.

So I called their hot-line at 5.45pm (good until 6.00 pm according to their documentation) and after 3 minutes of a recorded message, I get an answerphone! I leave a detailed message of my problem and await a response. Two days later I am still waiting so I try again. "The lines are busy", says the helpful switchboard operative who, after several minutes of my hanging on, agrees to take my details and to get someone to call be back. Another couple of days go by and I re-install the earlier version which compresses fine. I then call Centre Point once again and ask to speak to their customer relations manager, who is in "conference". I mention to the helpful woman who takes my call that I write articles for professional journals, etc., etc. Five minutes later I receive what I shall call a "pouring of oils on troubled waters" call from the head of their install base department. Lots of apologies about the lack of response, but with a new upgrade the phones are always busy, etc., etc. A solution to my problem is suggested however and I am pacified enough re-install the new version, which now works fine. As a footnote, I received a further response from Centre Point some two weeks after leaving my original message on their answerphone. They had only just got around to dealing with it and had not bothered to contact me in the interim!

My correlation between these problems is that in each case I was told that the help desk had been overloaded with queries. Well, why don't they take on temporary staff when they release a new version to handle the queries? Even if the extra help is non-technical, at least they could deal with the customer directly and ensure that a response is forthcoming, rather than leave their customer in the dark wondering whether the message ever got through. Likewise, if your company has a help desk, it may be worthwhile looking at the service level agreement it has with its customers and establish what they do when they release something new into the organisation.

Now on to more pleasant things. I spent an enjoyable few days at COMSEC 91 getting updated on all that's new on computer security. The keynote address was by Mustapha Ali Reda on the subject of "Business Resumption Planning in Kuwait". It was amazing just how much data was smuggled out of Kuwait after the invasion and how quickly they were able to resume processing because of this. It really bought a totally new interpretation as to what is meant by "off-site storage"! It does make you realise just how important your organisation's data and bespoke software actually is. Make sure that they take good care of it.

Finally, the season's greetings and a well controlled new-year to you all.

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 to discuss how you can get your name in print? (071-920 0111 extension 2342).

ANNUAL CONFERENCE

PRIORITY BOOKING

Turn to page 13

TickIT: Certifying Quality Management in IT

ALISON WEBB, INDEPENDENT CONSULTANT

WHAT IS TICKIT?

Computer auditors are only too well aware of what pitfalls there are in requisitioning a new computer system. Missed deadlines, unreliability, inefficiency and incomplete functionality are all traps for the unwary – and no matter how competent and experienced the purchaser, until now it's been almost impossible to be absolutely sure that the product or service you're buying does what the vendor says it does, except by trying it out. In 1989, the BCS estimated that losses due to poor quality software were costing the UK £2,000 million per year.

The problem of knowing if a product does what the manufacturer says it does isn't confined to the computer industry, of course: anyone who buys an electric kettle wants to be reasonably sure it won't electrocute them the first time it's switched on. The usual method of control is first to lay down standards which a product must meet, and then to give a certificate of approval to only those products which meet the standards. A customer can ask if a particular item of interest has the certificate, and if it does, what can reliably be expected of it. Typical examples of standards and certificates are the BSI Standards and the familiar kitemarks. Bodies in the UK who wish to issue certificates of this sort normally let themselves be vetted first by the National Accreditation Council for Certification Bodies (NACCB), and independent group with representatives from government and industry.

As a new industry, standards for computer systems have had to be developed from scratch, but BS 5750, ISO 9001 and the European harmonised Standard EN 29001 set out minimum best-practice requirements for organisations that provide, directly or indirectly, IT products and services. (Incidentally, these standards don't cover just computer companies: an advertisement for window blinds pushed through my letter-box recently claimed the company worked to BS 5750 . . .) The missing link until now has been an assessment system leading to the awarding of certificates geared specifically to the products of the IT industry – and this is what is provided by the TickIT scheme, sponsored by the DTI and managed by the TickIT Project Office. It will work in the same way as existing certification processes, using organisations accredited by the NACCB to carry out assessments and issue certificates. If they wish, existing Certification Bodies can apply to extend their scope to Tickit; before they are allowed to do so, the Council will carry out a competence check. Two such bodies have already been accepted: Bureau Veritas and Det norske Veritas; more are expected to follow.

Suppliers of computer products and services can ask for assessment and, if successful, prospective customers will know that their work reaches a certain measurable standard. (Those of us who worry that auditing is seen as a rather negative activity with not much of a product, will be pleased that Internal Audit departments can – and do – apply for certification.) TickIT is concerned with everything that contributes to the quality of what an organisation produces – the recruitment programme as well as the standards for system testing – so particular systems are not certified, rather the organisation as a whole. You may have seen the reports in the computer press when the first certificate was given to Logica.

WHAT IS THE ROLE OF THE AUDITOR?

Specialist auditors will carry out the pre-certification review on behalf of the certification body, who will either employ them directly or (more likely) contract for their services when reviews need to be done. Obviously, the organisations who want a certificate will vary: some will supply complete systems, including hardware, software and all support and maintenance; some will provide packages to run on a customer's existing software; and still others will provide specialist services like consultancy or training. A large group of companies with diverse interests may want just one facet of its business certified. Whatever the situation, each organisation will be asked as part of its application to define the scope of the activities it wants to include: for example, what sort of systems it supplies; to which industry sector; any specific architectures or operating systems it uses; any other services it provides. The audit is planned around this scope statement, measuring the performance of the organisation in each area against the detailed criteria set out in the TickIT Auditors' Guide.

Apart from helping with certification, it's expected that auditors with the TickIt qualification will work as "second parties" for companies considering buying-in systems, as well as Internal Auditors.

HOW TO BECOME A TICKIT AUDITOR

TickIT auditors need to be specially registered, and this is handled by the TickIT Office at the Institute of Quality Assurance. The registration criteria have been specified by the BCS, and three main requirements must be met:

(1) **Formal qualifications**

Ideally, a degree, although this may be replaced by appropriate training and experience.

(2) **Background**

You must have substantial practical IT experience, particularly in systems development. Experience in other areas such as engineering or accountancy is not acceptable. There is no need to have auditing experience: the necessary skills will be taught in a five-day course, which will be continually assessed and followed by a two-hour written examination, which you must complete successfully before you can be registered.

(3) **Experience**

Although provisional registration is possible after passing the course and an interview, registration will not be confirmed until relevant experience has been gained of assessing to a recognised Quality System Standard. Before full registration, work is performed under supervision.

If you're from an IT background and are already registered as an Assessor of Quality Systems with the National Assessor Registration Board, you will be eligible for registration as a TickIT auditor after an interview, although you must attend a 1-day seminar on TickIT documentation.

Detailed rules about entry requirements, information about training courses, and application forms are available in an Institute of Quality Assurance information pack. (Their address is 10 Grosvenor Gardens, London SW1W 0DQ, Tel: 071-823 5656).

MEMBERSHIP APPLICATION/RENEWAL?
See the subscription form on
page 15

Computer Security

Jim Kenney, Civil Service College

The computer security picture is a jigsaw completed by connecting the four pieces of procedural, personnel, physical and technical security together to form comprehensive protection for your Information Technology. In this article Jim Kinney, from the Civil Service College, looks at the concept of IT Security firstly by examining the drive towards technical standards for secure systems and secure products and secondly by encouraging the view that, although technical standards are important and topical, the wider issues involve people problems which are still the most difficult to manage.

The Scope of Computer Security

The relationship between business survival, both in the public and the private sectors, and the reliance upon Information Technology (IT) has become a real issue in recent years. A recent MORI poll[1] shows that senior management awareness of the importance of IT is improving. The following table indicates the relative importance of company concerns.

COMPANY CONCERNS	PERCENTAGE OF COMPANIES CONCERNED
Computer Security	41 %
Hostile Takeovers	35 %
Product Protection	26 %
Natural Disasters	22 %
Damaged / Lost Saleable Stocks	20 %
Fraud	16 %
Espionage and Information Loss	11 %
Protection of Executives	11 %
Malicious Damage	9 %

Although the specific issue of computer security attracted the largest level of concern, all other items in the survey have some relationship to the concept of computer security. This is because the security of any computer system is built around the principles of Confidentiality, Integrity and Availability (CIA). This concept can be summarised as being the extent to which the system:

- Preserves the confidentiality of the data, preventing the unauthorised disclosure of information.
- Protects the integrity of data, preventing the unauthorised modification of information.
- Maintains the availability of the data, ensuring the prevention of the unauthorised withholding of information or any data processing resources.

Technical Security Criteria

The concept of secure computer systems is a fairly recent phenomenon which was focused upon as a technical issue in 1985 with the publication, by the United States government, of the "Orange Book"[2] (although the history of the "Orange Book" can be traced back to 1967). When used in the context of IT the word security has a precise technical meaning relating to "trusted computer systems" and the criteria established by the Orange Book have been the driving force behind current standards for secure operating systems. The criteria were developed with three objectives in mind:

- To provide security standards for manufacturers to build into their products.
- To provide a matrix with which to evaluate the degree of trust that can be placed in computer systems for the processing of classified and sensitive information and where a product can be evaluated independent of an application environment or a system can be assessed with respect to its specific operational requirements.
- To provide a basis for the specification of security requirements in system development acquisitions.

The Orange Book was intended to be used in a government environment and is therefore heavily oriented towards the preservation of confidentiality and the prevention of data disclosure. In general the guidelines in the "Orange Book" revolve around security features which control and monitor access to information and six fundamental principles are identified:

- There must be a well defined SECURITY POLICY which is explicit in its requirements and in its enforcement.
- It must be possible to give a security MARKING to information.
- It is essential to IDENTIFY individual subjects and the levels of information which they are authorised to deal with.
- Audit trails in the system should ensure that actions affecting security can be identified and ACCOUNTABILITY established.
- The component parts of the system should allow the independent analyses which provide the ASSURANCE that the system enforce the prescribed security standards.
- The component parts of the system itself must be protected against unauthorised modification thus

ensuring the CONTINUOUS PROTECTION throughout the system life-cycle.

The criteria for trusted computer systems were divided into four divisions; "D" being the lowest, within divisions "C" and "B" there are further divisions known as "classes" and finally "A" which is the highest division. The criteria are ordered in a hierarchical manner and can be summarised as:

- Division D which provides minimal protection
- Division C which is discretionary protection based upon need-to-know and includes audit capabilities and accountability. The sub-divided classes are,
  - Class C1 which provides discretionary security protection, and
  - Class C2 which provides controlled access protection.
- Division B which enforces a set of mandatory access rules, sensitivity labels and a security policy model. The sub-divided classes are,
  - Class B1 which provides labelled security protection,
  - Class B2 which provides structured protection, and
  - Class B3 which identifies the principles of security domains.
- Division A which provides verified protection that assure that the mandatory and discretionary security controls used in the system provide for the protection of classified or other sensitive information.

European Technical Standards

In the United Kingdom the concept of computer security has been widened to include both government and the private sector, and where responsibility is maintained by the Communications-Electronics Security Group (CESG) who are mainly concerned with the "nationally classified" IT assets. Within the commercial sector the Department of Trade and Industry (DTI) has published the "Green Book" which is concerned with the protection of IT assets owned or held by UK industry and commerce. A third group, the CCTA IT Security and Infrastructure Group, is concerned with the protection of unclassified but sensitive assets within government. Within Europe much work has been done to build upon the UK standards and those of France, Germany and the Netherlands to provide a set of common, harmonised IT security criteria[3] resulting in the Information Technology Security Evaluation Criteria (ITSEC). These internationally harmonised criteria will provide a compatible basis for CERTIFICATION by the national bodies within the four co-operating countries and ultimately allow for a wider international agreement on evaluation results.

ITSEC deals with IT SYSTEMS and PRODUCTS, a system being a specific installation with a particular data processing purpose and operational environment designed to meet the requirements of END-USERS and a product being an "off the shelf" procurement which can be incorporated into the system environment. The criteria provide a selection of arbitrary security functions and operate within seven evaluation levels labelled E0 representing inadequate confidence up to E6 representing the highest level of confidence.

ITSEC uses the term TARGET OF EVALUATION (TOE) which will define and describe the security requirements and the solution to those requirements are laid out in a set of criteria for assurance evaluation. The evaluation criteria provide the SPONSOR of the evaluation (the person or organisation requesting evaluation) and the EVALUATION FACILITY (the organisation performing the evaluation) with the information and the necessary standards which are essential for particular CERTIFICATION.

The purpose of the ITSEC is to provide a wider range of possible systems and products than the "Orange Book" and provide a TOE with more architectural freedom. It is not possible to relate the evaluation levels directly between the ITSEC and the Orange Book but ITSEC does provide information of functionality classes which correspond closely and these are specified as F-C1 through to F-B3.

Wider Security Issues

Although the "Orange Book" and "ITSEC" primarily establish a set of technical security measures it is important to stress that computer security is a much wider issue and non-technical measures play a major part. Thus security also involves physical, personnel and the procedural controls which are established and administered within an organisation. The personnel issues in particular are vitally important.

Reported security breaches or computer fraud in large organisations makes headline news, therefore, there is a tendency to think that computer security surrounds the prevention of fraud and the detection of suspicious staff. However, it is the day-to- day problems of control in the IT environment, which although less spectacular in media terms, involves managerial time and effort to correct. In some cases personnel may not appreciate the implications of actions which they may take while working in an IT environment. Research in the United States[4] suggests that staff are largely trustworthy and that people involved in the development and use of IT would not take advantage of their privileged access rights, are generally responsible and overwhelmingly reject any behaviour that is disruptive or destructive. However, it is necessary to stress the importance of IT staff as an asset to the organisation. Essentially

- The responsibilities of IT staff need to be clearly defined in relation to other functional areas.

- There should be no conflict in the amount of IT work that should be performed and who should perform it
- The contribution that IT staff make to the organisation should not be undervalued and should be explicitly recognised
- Top management need to state clearly the policies of the organisation (particularly with reference to unauthorised software and personal use of facilities)
- System loopholes, i.e. internal hacking, may be sought and staff question the extent to which such behaviour is regarded as "nuisance".

It seems, therefore, that while there are many technical aspects to computer security the problems can be confined by sensible management of people. This highlights that computer security is a people problem and not merely a technical or a machine problem.

Availability Issues and Business Survival

A recent report[5] examined how well businesses could survive a major loss of IT services. The report revealed some interesting facts on business survival:

- Around 95% could survive with a loss of about 3-4 hours.
- 75% could survive a loss of between 0.5 and 1 day.
- Less than half of the companies could survive a loss of service of 2-3 days.
- Only 20% of companies could survive if IT services were lost for 2 weeks.
- Less than 10% could survive a loss of 1 month.

In a separate report[6] by a disaster recovery specialist 14% of IBM mid-range users could not maintain their business if they were to lose their IT services for more than 24 hours. The message appears to be, that while there is top management concern over computer security, there is still not the realisation the computer security is a vital part of the availability of IT facilities, and that means building in contingencies.

Much of the preservation of computer security has to be based around this contingency planning, i.e. if something goes wrong there are prescribed actions to put them right. This area of planning, also known disaster recovery planning or business continuity planning is principally risk based and can use a number risk management tools and methodologies. The method used for the unclassified area of government is the CCTA Risk Analysis & Management Method (CRAMM). CRAMM reviews are conducted in three stages:

- Stage 1 is the identification and valuation of system assets including data, software and physical hardware.
- Stage 2 identifies the level of threat and the vulnerabilities of the assets identified in stage 1 and measures the risk to your system.
- Stage 3 addresses risk management and the selection of cost effective countermeasures to reduce or minimise risk.

Part of that range of countermeasures is the effective use of Contingency Planning and creating system resilience. Total resilience, involving the duplication of all processing facilities may not be justified but a series of plans should provide reasonable protection such as:

- Standby arrangements which are periodically rehearsed.
- Dual processing facilities at the existing site to ensure essential processing.
- Off site storage for essential software and data.
- Physical protection of the existing site.
- Standby processing generators.

While these principles may be well established in the mainframe environment similar contingencies should exist at the user level and this is an essential part of business recovery or business continuity , i.e. within the systems developed by managers under their delegated responsibilities there will be critical small systems and data. Many users of small systems consider risk management inappropriate and therefore could not rely on any contingency measures for their systems. This is particularly important because it is evident that an increasing amounts of user processing means secure or sensitive data is being maintained at a micro-computer level and loss of this information or breaches of confidentiality of sensitive data could be embarrassing, or even commercially damaging, for an organisation.

Some Topical Security Problems

It is difficult to quantify the cost to organisations of lapses in computer security. Estimates of 400 million a year in direct losses have been reported[7]. However, indirect costs are more difficult to quantify, such as:

- Determining the extent of the security breach and repairing the damage to the system
- Rebuilding user confidence in the system
- Restoring organisational credibility

This is particularly so when resources are shared amongst many users and the security breach is in the form of a virus introduced into the computer system. There have been reported incidents[8] of virus attacks both in public and private sector organisations. One of the most common ways of viruses spreading is for users to use unauthorised software or to swap discs between different systems[9]. Significant number of staff, feel that the practice of sharing software is acceptable and this is part of the security problem of enforcing computer security policy and raising security awareness in organisations; a report suggests that forty per cent of companies (see reference 7) do not observe computer security policies. One method of controlling this problem is specific administration over the installation and use of vendor and application software in the office, with a general rule that users should have controlled access to information previously installed on hard disks[10]. Software and hardware solutions are available to provide the facilities for their systems administration in even the smallest computing environments with audit trails of system usage, system login's and password violations.

However, security breaches are bound to arise through the use of shared resources in a microcomputer based environment. Another general rule is that only authorised software should be installed by the systems administrator. One of the least highlighted problems problem associated with shared systems in that vendor based software is normally licensed as one copy per machine, however, due to the ease with which copies can be made this is a difficult area to control. There is always a risk, therefore, of a prosecution should a breach of copyright take place and there are instances where prosecution has taken place[11]. Lack of such things as inventories makes it a difficult and time consuming area for management to exercise control and it is difficult and time consuming to conduct comprehensive tests for likely breaches; it is important that an alliance is formed by objective third parties, such as Internal Audit and the Departmental Security Officer, in order that proper monitoring of system security is maintained. This would mean structured security reviews involving such things as:

- Detailed testing for compliance with organisational policies
- Cross checking against organisational inventories
- Quantifying the cost of security breaches
- Independent reporting to management or to security committees

Implicit in the protection of software is the protection of all data held on disk and the secure management of those disks, through accountability. This suggests that the individual who is responsible for system administration should also be responsible for the control of all magnetic media with general rules regarding back up and safe storage of copied data. One of the best ways of combatting the problems of computer abuse is in assigning proper responsibilities for data security. Analysis of this issue suggests that it is the users in the functional areas who should take this responsibility[13]. It is not only important to have someone in the office with primary responsibility for this role but also some secondary responsibilities should be placed on those who are given access to data[14]. Some users are familiar with access controls such as passwords but the storage of sensitive data will increase the need for access control consideration, such as authentication controls which limit individual access or authorization controls which limit access to particular operations[15]. In addition it is recognised that there are few standards and also general weaknesses in the development and maintenance of documentation to support user developed systems[18]. As microcomputer based systems become more sophisticated and their operations more complex the risks to the system increase. Users need to consider carefully the need for documentation to support the control of their systems, e.g. documented procedures for file backup or recovery instructions and contingency plans. This can be difficult for users who while at the same time as they develop the skills of "end-user computing" may lack the formal training in security. This is a growing problem as users move away from conventional, well controlled clerical environments, to third party based software such as word-processing or spreadsheet packages and this makes it difficult for management and for independent functions to monitor and evaluate the effectiveness of system usage.

Training & Awareness

There is a strong belief that users needed training in the security aspects of IT. Most organisations can provide some guidance to management and staff through their Information Systems Groups; this is usually on a consultative basis, mainly reactive, based upon user enquiries. In addition, Information Systems groups and the Departmental Security officers can issue guidance in both booklet form and through the use of staff circulation notices to increase awareness. All of the above must be supported from the top through defined policies and by documentation which contains statements of the policy and instructions and guidelines on how data security should be dealt with. The Civil Service College provides formal training[19] in security and audit, for both the public and the private sector, in all of the areas described in this article but it must be stressed that the provision of "in house" training by organisations themselves is also essential to maintain an awareness of computer security across the whole of the organisation.

REFERENCES

1. Smith, D, Computer Systems Disaster Report is Unequivocal: Plan Now or Risk Corporate Roulette, Information Technology and Public Money, Vol 9 No. 1, 1990.
2. The Department of Defense (DoD) Trusted Computer System Evaluation Criteria, DoD, 5200.28-STD, December 1985.
3. Information Technology Security Evaluation Criteria (ITSEC) - Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom, Version 2.1 (Prov) June 1991, Dept. of Trade and Industry / HMSO 1991.
4. Paradice, David. B., Ethical Attitudes of Entry-Level MIS Personnel, Information & Management 18 (1990).
5. Amdahl Executive Institute (AEI), Computer Disasters and Contingency Planning 1990.

6. Financial Times Business Information Issue 172.
7. Survey of computer security by Dr. Adrian Warman of the London School of Economics, reported in the Daily Telegraph 5th Aug. 1991.
8. The Daily Telegraph, Dec. 1990 carried a report of a computer virus which affected a computer system in the House of Commons Library.
9. Sophos Ltd and Airtech Security Ltd., Viruses on Personal Computers - a Growing Threat, Abbey Press (1990) p13.
10. Ibid, p43.
11. Athey, Susan., Software Copying Politics of The Fortune 500, Journal of Systems Management July 1989.
12. Datapro Reports on Information Security, An Alliance: EDP Auditing and Information Security, Datapro Research, April 1990.
13. Courtney, Robert H. Proper Assignment of Responsibility For Data Security, Security, Volum 11 No. 2 April 1989 p83.
14. Ibid, p84.
15. Hansen, James V & Romney, Marshal B, Data Base Management Controls for Microcomputer Systems, Internal Auditor, Dec. 1987.
18. Ibid
19. Civil Service College Prospectus 1991 - 92, p86 - 87.

SUBMISSION DEADLINES

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

An Introduction to Auditing MVS

Alan Oliphant

The subject of the meeting held on 21st October 1991 was 'Auditing the MVS Operating System'. It was originally planned that this should be given by Alan Oliphant, Computer Audit Manager with The Standard Life Assurance Company. Alan has been involved with computing since 1973 and has been a computer auditor with many diverse companies on several continents since 1975. He is currently Chairman of the Institute Of Internal Auditors IT Audit Development Committee and is actively involved in organising the annual COMPACS conference.

Unfortunately Alan was unable to give the presentation and was substituted by Mike Kerford-Byrnes. Mike is an independent systems consultant with many years experience of IBM operating software.

The presentation and its accompanying documentation was based on a research report recently produced by the IT Audit Development Committee of the Institute of Internal Auditors. Full copies of the report can be obtained from:

The Institute of Internal Auditors
13 Abbeville Mews
88 Clapham Park Road
London SW4 7BX

Auditing MVS can be a very complex procedure, so the presentation did not attempt to describe the process in detail. Rather, it was intended to provide an introduction to the reasons for auditing the operating system and to suggest a way in which auditors new to this type of review could approach the area in a competent manner.

Mike's presentation covered some extremely interesting new areas, including:

System Parameter Library

This is the library which contains most of the control information for MVS at system initialisation time. The features of this library and the items to be checked were described along with their significance.

Authorised Program Facility

The APF is the single most important feature within MVS and allows programs to work outside the normal constraints of operating system security. It is therefore vital to find out which programs can run outside normal security, determine how they themselves are protected and to analyze the programs to determine their functions. This is one area where even experienced computer auditors may find difficulties, given that the specialist expertise necessary to analyze Assembler code is not common in the auditing community.

Program Properties Table

PPT is another fundamental control feature. This table describes to the operating system those programs which require special properties when they are run. It can grant programs special powers and must be checked during audits of MVS.

System Management Facility

SMF provides an audit trail for MVS. However, it is not an easy trail to analyze. To complicate things even further, the type of entry in the trail is often optional. It is extremely important for auditors to ensure that all significant events are being recorded and that audit trails are adequately protected. Exits are also provided within the SMF processing to allow user definable code to be processed at specific points during SMF processing. The use of exits requires special scrutiny as the code executed here is effectively outside the control of any security function.

Job Entry Subsystem

JES is the part of the operating system which controls the workflow of the system and organises the output. Like SMF, exits exist within JES for user defined code. Again, this exit code must be subjected to scrutiny. Operators can issue commands to JES for a variety of functions. Unless specifically restricted to the system console, these commands can be entered from a variety of sources with diminishing levels of control.

Supervisor Calls

SVCs are the main method of communication between MVS and programs. SVCs are specific programs which request specific services such as opening datasets etc. Some SVCs request very sensitive system functions and need to be protected.

Conclusion

This was an interesting and useful presentation, very professionally delivered by Mike. 'How to' papers like this are the backbone of professional interest groups like CASG, where auditors and other specialists can share their knowledge and skills, and help to give confidence and support to colleagues.

ADVANCE NOTICE

casg
Computer Audit Specialist Group

Annual Conference

Wednesday 13th May 1992

DISASTER RECOVERY - AN AUDIT PERSPECTIVE

"Without the support of our computer systems we would continue trading for only a few days before losing control of our business". This is the view of many chief executives and finance directors today.

What would happen to your business if your data processing centre vanished in a puff of smoke, or was drowned in a tempest? A question most of us try not to think about.

In the modern business environment we have become increasingly reliant on the safe and uninterrupted functioning of our computers. Given the importance of IT to our company's operations it is surprising that Contingency Plans are neglected, untried and untested.

At our annual conference we will be exploring the whole area of Contingency Planning. Our Speakers have been chosen to give delegates a sound understanding of the topic. During the course of the day you will hear from a consultant who specialises in the formation of Contingency Plans, from an internal auditor about how to test the plans, from a company that has suffered its own disaster and the lessons learnt, and from an expert who will tell us what services are available.

At the end of the conference you will be able to go back to your company and be able to address the issues of Contingency Planning with confidence.

VENUE: The London Press Centre
76 Shoe Lane
London
EC4A 3JB

The fee for the conference, which includes conference papers, coffee and lunch will be:

BCS or CASG Members	£150
Non Members	£200

The non-member rate includes automatic corporate membership of CASG.

Please complete a membership application form and return it with this booking)

BOOK YOUR PLACE NOW BY COMPLETING AND RETURNING THE SLIP OPPOSITE

casg
Computer Audit Specialist Group

The British Computer Society

ANNUAL CONFERENCE - PRIORITY BOOKING

To: Mr A J Thomas, 3 Kings Court, The Maltings, Great Dunmow, Essex, CM6 1UX

DISASTER RECOVERY - AN AUDIT PERSPECTIVE

I enclose a cheque for £.................. being fees for .... delegates for the annual conference.

Please register the following bookings:

1. Name: ....

   Position: ....

   Company: ....

   Address: ....

   Telephone: ....

2. Name: ....

   Position: ....

3. Name: ....

   Position: ....

4. Name: ....

   Position: ....

5. Name: ....

   Position: ....

casg

Computer Audit Specialist Group

CONFERENCE PROGRAMME

13th May 1992

The London Press Centre

76 Shoe Lane, London EC4A 3JB

DISASTER RECOVERY - AN AUDIT PERSPECTIVE

0900	Delegate Registration	
0925	Chairman's Introduction	John Mitchell Chairman CASG
0935	The Consultant's Role	Speaker from a consultancy firm providing Contingency Planning
1035	Coffee	
1105	The Alternatives	Alan Bell Amdahl Executive Institute
1205	Lunch	
1330	Experiencing a Disaster	Speaker to be confirmed
1430	Tea	
1500	Testing the Plan	An Internal Auditor
1600	Panel Session	All Speakers
1516	Close	

1630 The Annual General Meeting for 1992 of the Computer Audit Specialist Group will take place in the lecture hall.

casg
Computer Audit
Specialist Group

The British Computer Society

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

Membership Application

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	4 = Academic
2 = External Audit	5 = Other (please specify)
3 = Data Processor	

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:

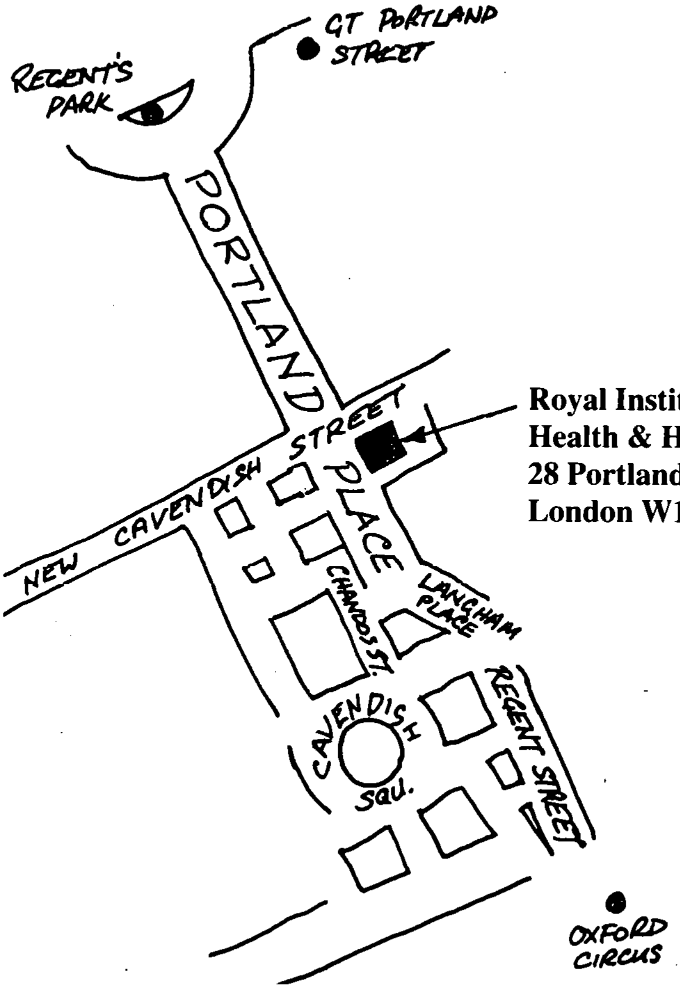
ADDRESS:

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



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

Printed by City University Print Unit