ISSN 0961-9348

The British Computer Society

Journal

AUTUMN 92
Volume 3, Number 2

Members' Meetings for 1992/93

1992		
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**	Rob Melville City University Business School Leslie Willcocks Templeton College, Oxford
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 if you have not already done so.

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 Autumn issue of the Journal continues the balance of articles between topical, future and practical themes which is our editorial policy. This variety is what makes the editorial chair such an interesting position. As a practising computer auditor, there is always the trap of the immediate present where the real need to review current systems conflicts with the desire to prepare for the future. The auditing profession cannot afford to be left behind by new technology, yet in the midst of this terrible depression (we are not facing the truth if we continue to call it a mere 'recession') there can be few organizations with the ability to spare staff time for training and research. In the face of this, high quality and readable papers which focus on the issues which are facing us all become invaluable. But do not let these issues remain unquestioned; our journal is the key focal point for specialist computer auditors, correspondence and dialogues will extend and expand our knowledge to the benefit of our profession.

• • •

With the recent batch of examination results from a wide range of bodies (IIA, CACA, ICA, EDPAA and several others) it is time for me to continue a theme started by John Mitchell in a previous issue: why are auditors so computer illiterate? Obviously, specialists from technical disciplines have the benefit of their experience, so programmers understand programming, analysts can relate to developing systems, and project managers know how to convince users that time and money budgets can be magically transformed into fairy stories . . . It is the generalist who is my biggest worry, the well motivated accountant or manager who moves into internal, external or computer audit with sound business and practical skills but a relationship with IT which should have disappeared with the end of the last decade. As someone who is involved in teaching computer audit in several institutions, I am extremely concerned that the wider profession of auditing (external and internal) is not developing genuine computing and IT skills. We are in danger of recreating the bad old days where specialist computer people work separately from generalists, and many auditors simply ignore the need for computer literacy at all.

So what can we do?

To begin with, we need to improve the quality and quantity of computing and information processing textbooks aimed at business users, rather than specialists. My summer project was to read and review several huge (800 pages plus) IS/IT and information management texts. Some were gloriously laid out, with full colour pictures and lots of useful details and case studies. Others were not as glamorous, but conscientious guides to all types of information systems. So what was the problem? Quite simply, they were all from the USA and geared to their educational system and all the examples were related to specific USA problems. Apart from Andrew Chambers and John Court, there are hardly any readable and useful introductions to computer audit. For our next year's objectives, perhaps members can suggest ways in which we in computer auditing can enable our generalist colleagues to achieve literacy and competence. At the very least, we will make a lot of examiners very happy.

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, what a summer it's been. Your committee has slaved their respective intestines out to produce next season's programme, which you will have received with the summer mailshot. Hopefully, you will have paid your subs and be looking forward to attending our first meeting of the new season where William List will, no doubt, be his usual controversial self when dealing with EDI.

* * * * *

On that subject I know of one organisation where the stuff came in over the wires from the New York office, popped itself into the mainframe and then made its way onto a micro for subsequent processing. As this was the first live run the chief accountant, who was an old IT hand anyway, insisted on a full reconciliation between the paper in the New York office, the mainframe records and what was on the micro. Surprise, surprise, nothing tied up at all. Upon checking with the IT department it turned out that they had never done a full parallel run and hadn't really bothered to educate the New York end anyway. The accountant was upset, but my question was, "what was user management doing when this was under development"? Lots of excuses were forthcoming, lots of finger pointing took place, but at the end of the day it was obvious that there was no real managerial control being exerted over system development. Just when will organisations learn that control is a managerial responsibility?

* * * * *

Wessex Health Authority has been getting some bad press for a long time and the latest District Auditors report has finally blown the thing wide open. Watch your I.T. tendering processes carefully if you want to keep your company out of the computing and national press, is my advice. Wessex fell down on the corporate governance side as did Atlantic Leasing, BCCI and the Maxwell Group. Stepping aside from pure computer audit for the moment, and dealing with wider audit issues, the draft Cadbury report on corporate governance makes interesting, if somewhat depressing reading, for all internal auditors. If you haven't seen it yet, you should have done, as comments were required by the end of July. The final report is due out in November. Make sure that you get your copy.

* * * * *

I sometimes get asked to speak at security events and tend to disappoint the audience by dealing with managerial issues rather than the latest technology gizzmos. They look even more glum when I point out that security is simply a sub-set of the overall control regime and that if they spent as much time and money implementing a structured control methodology as they did in security gizzmos, they would probably save a fortune in eliminating mistakes. Unfortunately, most of the audience are "security" officers, rather than senior management. I sometimes think that I only get invited on the basis of being the equivalent of a middle ages (or aged) court jester: "isn't he amusing, but doesn't he talk a load of rot, not like all these other nice people who use long technology words to explain how complicated everything is and thus secure our jobs for us". I really am getting even more cynical in my old age, than I was when I first started in audit. I just hope that there isn't a cure!

* * * * *

I refuse to write anything about Windows 3.1 this month. My spell checker doesn't recognise some of the words that I would use!

I look forward to seeing many of you in October.

The 'Lights Out' Datacentre Today? Tomorrow? Ever?

John James
Amdahl (U.K.) Ltd.

When data centre managers get together, we can be sure that (as with all professional groups) the industry buzzwords will fly thick and fast. One of today's favourite issues for discussion is the 'lights out data centre'. The words said and written on this subject are becoming so numerous that any data centre manager who has not yet taken the 'lights out' route might be forgiven for thinking that he or she is somehow failing to keep up with a key industry trend.

Yet the fact is that 'lights out' is not universally accepted as the only way forward; indeed, there is a great deal of disagreement as to what the term actually means in practice. This paper attempts to clarify the situation, and, along with some historical background, to address the questions:

- What does 'lights out' actually mean? And while we're at it, what do the terms automated, remote, and unattended mean, in the context of computer data centre operations - are they the same, or different, or related somehow?

- What will happen in the future with data centre operations technology? Will everyone be adopting the 'lights out' (whatever that means) approach, or will sites with different requirements be using different solutions for their operations needs?

We shall see that the term 'lights out' is not a particularly useful one, and that data centres, in practice, adopt specific techniques (such as automated and unattended operation) to suit their specific needs. This will continue to be true in future, although technology will make it easier for data centre managers to implement the solutions that are required. The 'focal point' operations facility of the future will render data centre operations more accurate and more repeatable, and yet, at the same time, more fulfilling for those who work in the data centre.

WHERE DID WE COME FROM?

Let's start out by examining where today's data centre procedures came from. Consider the job of computer operator in the early days of System/360. The operator sat directly in front of the processor; to the operator's side were the switches and lights that were used for 'hardware' control (start, stop, initial load, modify storage contents, and so on). In front of the operator was a typewriter device, used for communication with the software elements of the system: the operating system, the database and job management subsystems, the applications themselves, the batch job scheduler, etc. Very quickly, the typewriter became a visual display unit (the 'console' device that we know today) and the lights and switches disappeared and were replaced by VDU functions; the operator had a mode switch to jump between hardware and software control.

As workload levels grew, this single point of control became crowded as several operators jostled in front of the processor, so data centres began to install specialised software control consoles in such parts of the computer room as the tape area, the printer area, and the network control area. Most large sites installed two or three processors, and each of them needed these multiple operating consoles. In addition, there was a need for specialised consoles for performance monitoring, database subsystem control, and more; pretty soon, there were more console screens scattered around the computer room than there were people to monitor them.

BRIDGE OPERATIONS

Many large sites responded to this problem by adopting a 'bridge' approach to data centre operations, the main attraction being that the bridge allowed many of those consoles to be gathered together in one place, with perhaps some rationalisation being done. Most of the Operations staff could now be accommodated in an area designed with the needs of humans, not machines, in mind.

The classic bridge, of course, looks like a ship's bridge - a glass-fronted area, often raised, at one end of the computer room, from where Operators can survey the humming boxes under their control. If all the 'manual' computer room activities such as mounting tape reels and servicing the high-speed printers were consigned to side-rooms outside of the main computer room itself, then there was no need for anyone at all to be in the computer room in the normal course of events. And this was a good thing, because humans beings are, after all, not good news in a computer room: they create dust, smoke, and debris; they walk about and create vibration; they bump into things; they complain about the noise of the computers and the low temperature that has to be maintained. So it was not long before sites began to turn the lights out in the computer room itself - no humans in there, why pay to have the lights on?

A bridge does not have to resemble a ship's bridge. Some sites established their bridge in a separate room close to the computer room; or on another floor in the same building; or in an adjacent building. Whatever solution was chosen, the principle was the same - get as many Operators as possible out of the main computer room.

So is this 'lights-out' operation? Not really. In this situation, we still have a full complement of Operators, who are in (or close to) the data centre building; some of them are still in there, in side-rooms, servicing the tape drives and high-speed printers; the data centre is still 'manned' in practice, and the actual processes and procedures of operating the computer have changed little since the early days.

AUTOMATED OPERATIONS

Data centre operations did start to change, however, in the 1980s, and the change process has accelerated noticeably in the 1990s. This change is known generally as 'automated operations', although some people, worried about the implications of telling staff that their jobs are going to be 'automated', prefer to talk about 'assisted operations' or 'advanced operations' (all of which contract conveniently to the same initials, AO).

The move to automated operations has a number of underlying causes. Cost was one factor: a typical mainframe computer today is probably one hundred times more powerful than the typical model of twenty years ago - without some rethinking of operational practices, data centres today would be employing massive numbers of people just to keep up with the operational demands of the processor. And these people do not come cheap; the data centre needs skilled technicians with in-depth experience of the particular products in use and of the specific computing services that are being delivered. This would be a serious issue in any industry, but in IT is made more acute by the sector's notoriously high level of job mobility.

Another major issue has been job satisfaction. What self-respecting professional would want to stay in a job involving trivial repetitive tasks that could obviously be done better by a machine? Trying to cope with the complexity of scanning several console screens for important messages (with each console producing dozens of messages each second, the majority of those messages being of no interest to anyone at all) is hardly a recipe for job satisfaction for an experienced Operator. No wonder then that many automation projects have started by simply examining the processor's message output and eliminating that vast majority of messages that do nothing except clutter up the console screen.

But the most important driver in the automation movement is probably the dual need in the data centre to cope with an increasingly complex technical infrastructure while at the same time delivering ever more reliable and available computing services. We noted above that mainframes have become more powerful (and, indeed, will go on doing so); they have also become considerably more complex to operate at the levels of both hardware (e.g. the ability to perform the dynamic split of a multiprocessor complex in the event of component failure) and software (mainframe data centres today are expected to run more applications and subsystems than ever before, each one of them with its own - usually unique - operational interfaces; and the fact is that today's online applications, based on database subsystems and telecommunications, are more complex than the traditional batch applications of twenty years ago).

It would surely be unrealistic not to expect human error to become a factor in such an increasingly complex environment. And yet the data centre's clients (the end-users of the computing services) are increasingly unwilling or unable to tolerate breaks in service as the enterprise's basic business functions become more and more dependent upon IT. Automation in the data centre addresses this apparent dichotomy, firstly by reducing or eliminating human error in computer operations, and secondly by pro-actively monitoring end-user service levels to provide early warnings of performance and availability shortfalls.

Automation can take many forms, including the use of robotic devices to mount tape cartridges; the elimination of unnecessary console messages; the implementation of computer-maintained batch workload schedules; the introduction of automated linkages between different application systems (e.g. the successful creation of a particular file automatically results in the initiation of application program suites that use that file); the use of automated storage space management tools; the development of automated reactions to error situations (such as job failures or network problems); the use of automated problem and change management systems; and the use of automated performance and service-level monitoring and management systems. That is, automation can potentially address any data centre activity or event which could otherwise be subject to human error, or which could adversely impact the service levels provided to end-users. Every data centre will have its own view on which activities are the most important, and therefore where work should start and how automation projects should progress over time.

So does automation equate to lights-out? Once again, the answer is 'not really'. Automation is almost certainly a prerequisite for a lights-out environment, but to automate a site does not necessarily mean eliminating all the people; the extent to which automation is adopted in a specific data centre will depend upon that data centre's requirements. Some data centre managers will tell you that to eliminate people is not their goal – they have already reduced headcount significantly, and are now more interested in being able to handle more complexity and increased computer workload levels with the staff that they have left.

REMOTE OPERATIONS

Remote operations is another 'in' phrase. What it means is that a data centre is operated by people who are located some distance away (as opposed to the traditional setup, where the operations staff are in, or close to, the computer room).

The use of a remote operations solution may come about as a result of an enterprise deciding to consolidate its many centres of IT technical expertise into one place (perhaps as a result of a corporate reorganisation, consolidation, or takeover). Mainframe data centres do not only need computer operators; they also need other expensive professionals such as operations support staff, help desk staff, systems programmers, hardware and software planners, and so on. Many large companies that have traditionally maintained several data centres, each with its own complement of experts, are now reconsidering this strategy. They may decide to centralise the IT expertise at headquarters, but to keep multiple physical data centres for reasons of strategy or contingency.

Alternatively, we have seen other organisations that have only one mainframe data centre, deciding to build a second one some distance away. Again, contingency requirements can be a driving force here; or the data centre may simply need space to grow, and that space may be much cheaper to acquire in some rural location away from the company's downtown HQ. So let's move all or some of the computer equipment, but let's leave the people at HQ and avoid staff disruption.

A remote operations environment will usually come in one of two forms.

Firstly, the main data centre may be manned in the traditional fashion, and the operators on the bridge there have all the necessary console devices to be able to operate the processors at both the local and remote data centres.

Alternatively, the operations bridge may be located remotely from all the data centres (e.g. the bridge is downtown, while all the data centres are located in the countryside).

In both cases, the 'remote' data centre (or data centres) will typically be running with its computer room dark. So is this 'lights-out' operation? Well, probably not. The remote data centre is, after all, 'manned', albeit from a distance. Even though the operations staff may be many miles away, the processor still has the ability to call for help via its consoles if it needs advice on how to recover from unusual events such as a job failure; indeed, some organisations have achieved a remote operations environment with very little in the way of automation having been done.

Also, many so-called remote operations environments are not wholly remotely operated. Some companies choose to have a skeleton staff at the remote data centre (often to look after the tape drives and tape cartridge library – otherwise some other solution to the remote site's data storage needs would have to be provided, possibly at considerable cost). There is nothing invalid about this: each company must adopt the appropriate solution to its needs based on the amount of resources that it is prepared to invest, and a semi-manned solution is perfectly appropriate in many cases. Even if there are no technical staff at the remote site, the organisation must satisfy itself that appropriate measures have been taken in the areas of physical security and environmental monitoring, and the presence of security staff is sometimes deemed desirable; otherwise, the appropriate monitoring equipment must be capable of raising the alarm at the distant operations bridge, or some similar remote functions must be in place.

UNATTENDED OPERATIONS

Unattended operations means running the mainframe data centre without any staff in attendance, either locally or at a distance. Consequently, in an unattended environment there is nobody present to monitor console screens, or to mount tape cartridges, or to attend to the high-speed printers when they run out of paper, or to pick up the help desk phone when an end-user calls with a problem.

In an unattended environment, therefore, all activities which were traditionally manual tasks must be eliminiated or avoided. Traditional tape devices must be replaced by costly online disk storage, or by some robotic tape facility. High-speed printing in the data centre must be eliminated, perhaps by moving the printers to the end-users' locations, or by leaving all reports 'on line' so that end-users can view them through their desktop terminals, instead of receiving them on paper. Security and environmental monitoring products should be installed, which, in the event of an alert, automatically dial-out to alarms installed at the duty managers' homes or at specialist third-party premises.

Similarly, all non-manual activities must be eliminated or avoided. Therefore, there will be no point in the processor producing any 'action' messages on any console screen; there will be no point in any application program producing a message such as 'enter today's date' – a kind of event that used to be a very common occurence in data centres; there will be no point in the network control system asking for diagnostics to be run on a telecommunications line which has just failed; and so on. If a catastrophic event should occur (e.g. the failure of the operating system or a major subsystem), then it must be automatically recognised and treated like the 'manual' activities above: facilities must be installed

to dial-out to a duty manager who will take some remedial action (perhaps by connecting to the processor from a PC at home, and entering the appropriate hardware and software commands to bring the system back on the air). All the components of such an unattended environment are available in the marketplace, at a price, and can be used to build the operations capability that the organisation seeks.

This is probably the only true 'lights out' environment. Automated operations is clearly an essential prerequisite for this environment, but equally essential are a thorough understanding of every data centre activity and process, and a complete rethink of the way that the data centre is organised and managed. These are very onerous tasks, and it is generally accepted amongst data centre managers that unattended operations is a major step to contemplate.

Some organisations have therefore adopted an approach that says that the data centre only needs to run attended for some specific period during each 24 hours. Perhaps as a result of severe staff shortages, a data centre may choose to run unattended overnight but attended during the day, and so make optimum use of scarce human resources. The advantage of this approach is that not all manual tasks necessarily have to be eliminted; they could perhaps be rescheduled instead. Therefore, services such as tape cartridge mounts and high-speed printing could be offered, but only at daytime; there would be staff manning the help desk as normal during the day, with an answering machine working instead overnight. Once again, it all depends upon the needs of the particular enterprise in question.

WHAT ABOUT THE FUTURE?

As technical skills become more expensive and more scarce, and as the end-user community's requirement for very high levels of computer service availability continues to become ever more stringent, we can expect to see more and more data centres adopting automated operations techniques during the 1990s. Whether automation is regarded as an end in itself at a particular site, or whether it is seen as one step on the road to remote or unattended operations, will continue to be a decision for the individual data centre. The difference in the 1990s will be that the tools needed to build these more sophisticated environments will be easier to acquire and to use; and the chief amongst these will be the 'focal point' facility.

The focal point concept is essentially that a mainframe computer should be controlled, not by its own programmed logic, but by a separate, smaller computer, which provides the interface to operations. The way that such products will work will not be to take over the tasks currently done by existing AO products (therefore, the first level of automation processes will still take place as close to source as possible), but rather they will provide an additional level of operations management which complements improvements already made.

A focal-point product will typically be installed and used in a bridge environment, providing an improved technical capability for a data centre which has already centralised its point of control. The functional characteristics of focal-point products will generally include the following:

- Advanced human interface: the "WIMP" interface ('Windows, Icons, Mice, Pointers') will typically replace today's clumsy line-by-line typing method by which the operator communicates with the mainframe computer. WIMP is an advanced ergonomic facility already in use on modern workstation computers; it reduces the number of keystrokes required to enter commands, and uses menu driven techniques to reduce the potential for the operator to make typing errors;

- Automation platform; anything that can be timed (time of day, or time period elapsed) will be done by the focal-point computer; there will be scripts to replace today's lists of commands entered in longhand;

- Rule-based logic: the automation logic will include a rule facility so that the manufacturer and the data centre staff can easily and quickly modify and extend the functions performed by the focal point;

- Online documentation: all documentation about the focal point itself, and the control functions of the mainframe computer, will be held in the focal point itself and will replace today's paper manuals;

- Graphical capability: the focal point will collect statistics about the performance of the attached computers and will use its advanced graphical capabilities to massage, format and display the resulting information;

- Automated configuration facilities: many, or all, of the configuration tasks which have to be performed for a large-scale mainframe computer (by the manufacturer's field engineer at installation time, and subsequently by operations staff, when resources have to be reconfigured in failure situations) will be done through the focal point, and records of changes made will be kept automatically;

- Product independence: because it will provide a common interface to many different products, the focal point will allow the introduction of new products to be disguised from operations staff, so that for operators and field engineers alike, the learning curve associated with new computer products will be reduced or eliminated;

- Testing facilities: the focal point will include the ability for operators to test new functions by 'dry running' them, without impacting the production computer workload.

The rule-based logic and the automated configuration facilities in the above list of characteristics will eventually allow the introduction of artificial intelligence into future focal point products. The term artificial intelligence applies to computer systems that can collect and assemble data so as to be able to reason and perceive. One application of AI is expert systems, which can be defined as applying to acquired knowledge of a human expert to the solution of a problem (the difference between today's rule-based logic and tomorrow's expert system being that the expert system can operate on partial or 'fuzzy' data). In the case in point, the problem to be addressed is the efficient operation of a mainframe computer. Such a facility is required, not just because of the repetitive nature of much of a computer operator's work, but also because of the sheer complexity that threatens to overwhelm operators.

The focal point's rule-based architecture will provide the basis for the knowledge representation that an expert system requires (that is, the rules that are followed to solve a problem or to set out a plan of action), which its configuration facilities will form the basis of the knowledge base (i.e. the body of information about the data centre and its characteristics), which is the remaining component needed for an expert system. What is needed to complete the expert system environment is the ability for a problem to be recognised automatically, and for the solution (once it has been worked out) to be communicated automatically to the mainframe computer under control. The interfaces which the focal point will have to all installed mainframes in the data centre will provide these missing capabilities.

In summary, the focal point concept is all about recognising problems quickly, and ensuring that the data centre's standard reaction to a specific problem is automatically invoked wherever possible. The focal point will therefore improve the quality of the operations processes that are undertaken in the data centre; for those data centre managers who want to go further into remote and unattended operations, the focal point's ability to connect to multiple mainframes, and its decision-making capabilities, respectively, will prove to be useful features.

THE AS400 AUDITING HANDBOOK

M Lindsey – Computer Auditor, Argos plc

This Handbook is now available. The main benefit of the book is that it is essentially a book about "learning through doing" and, therefore, should interest those auditors reviewing the AS400 environment for the first time.

Technical tests are explained in detail. A suggested audit approach and a recommended audit plan is included together with approximate timings that you may expect for the audit processes.

I am particularly fortunate to have the benefit of an editor who is an expert on the AS400. Neil Hare-Brown has had experience in the Information Systems Audit group of the National Westminster Bank and, previously, as a consultant with BIS Banking Systems International Limited.

I hope that the Handbook proves to be a useful contribution to AS400 auditing and look forward to feedback in this respect.

THE AS400 AUDITING HANDBOOK

Author: Malcolm Lindsey

Editor: Neil Hare-Brown

Cost: £3.75 plus 50p p&p

Please send your name, address and cheque made payable "BCS CASG" to:

M Lindsey
4 Cossett Green
Hemel Hempstead
Herts
HP3 8QP

Open Systems: An Introduction

Craig Arnall
KPMG Management Consultants

Craig Arnall of KPMG Management Consultants highlights the importance of Open Systems, which is emerging as a very popular computing technology. It is important that accountants are aware of its potential. Equally, we need to understand its drawbacks. As with all such technologies, there is a wealth of jargon, which can lead to confusion. Open Systems is more than a technical issue. It can have a profound impact on the way businesses operate. This article is therefore addressed to those with reponsibility for commercial decisions about the use of computers rather than those who make them work.

Open Systems is a topic of concern for accountants: for those with departmental responsiblity for computer systems; those who approve spending plans; and those who wish to streamline business operations, for example through automating order processing, invoicing and payments.

The basic idea of Open Systems is that suppliers of different system components should build them to commonly agreed specifications. The approach has been proven for the desktop Personal Computer, with the whole software industry able to develop applications that run on many different hardware vendors' equipment.

This idea of being able to join together different elements of a system which are obtained from many sources is commonplace in most engineering disciplines. In the construction industry, for example, architects develop designs for building interiors with the confidence that electrical, heating, lighting and ventilation systems can be installed by different sub-contractors. Once installed the various elements of a building are expected to work together smoothly. The basis for this expectation lies in well-established standards for the characteristics of components, so suppliers publish clear specifications and architects can confidently design for their integration.

In a more familiar example, financial systems are often bought as software packages that provide a complete set of functions – general ledger, accounts payable, accounts receivable and order processing. Most companies buy the different modules from a single supplier. Such an approach is generally easier for the user because screens and reports have a similar appearance throughout the range of applications. The onus is put on the supplier to integrate the systems properly, for example by ensuring that postings between different ledgers are carried out accordingly.

Although this approach works for small companies with straighforward needs, it can cause problems for larger organisations. Groups of companies may find that different parts of their business need the features of different suppliers' products. Similarly, a company might wish to choose an order entry package from one source and ledgers from another. The usual solution is either to compromise and choose a single supplier or to carry out manual reconciliation between systems. Open Systems offer purchasers the potential to choose the best modules for their particular needs and to integrate them to provide a complete solution.

The approach lies on common standards. At the information level, different components must support the same structure for ledger codes and the chart of accounts. For users, standard screen handling mechanisms allow the same look and feel to be provided for diverse underlying software applications. Systems may need to run on different hardware platforms, maybe with one type of computer for order entry and another for finance applications. Finally, there will often be a need for communcations standards so that the different systems can exchange data. These are largely technical issues and, by and large, those with responsibility for procurement decisions will not wish to know about the detail. However, they will wish to be assured that their selected supplier is working to established standards.

The introduction of Open Systems standards provides a stable technology infrastructure, so that new application systems can be introduced without requiring changes to everything that is already in place. Skills are retained because technical staff are working with common tools, so allowing greater choice and flexibility in choosing different solutions. At the technical level, the approach means that software applications can be *portable*, running on different vendors' hardware. Applications can be *scalable* – capable of working on a range of hardware, from small desktop systems through to mainframes according to needs and company growth. Applications can *interoperate*, so that information is shared between different systems and they can work together coherently.

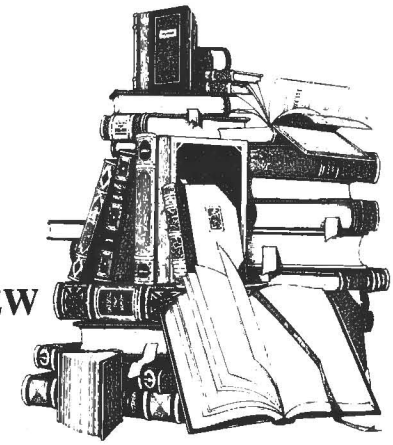
The computer industry is making significant progress in realising the potential of Open Systems. All major vendors now supply 'UNIX' systems, which provide a common operating environment across all their equipment. Although there are many variants of

UNIX they have much in common and are gradually being aligned with one another. Similarly, standards for communications have been developed – both at the base networking level and also for high level communications such as Electronic Data Interchange for transmitting purchase orders, invoices and payments between trading partners.

In time, common standards will improve customer choice. Greater competition is already driving down costs in the consumer's interest and this trend can be expected to continue. Greater use of standards also helps combat a common problem, in which a company is easily locked into a single supplier because of historic investment in equipment that would be too expensive to change.

A number of problems still remain. Some observers believe that Open Systems has been over-promoted as a panacea for all computing problems. Although many of the necessary products are available, they are still not fully mature. However, companies can make valuable first steps by investigating the technology and buying products where suitable ones are available. In many cases this will lead them only part way towards the full potential benefits of Open Systems – but their initial purchases and the experience gained will put them in a position to achieve far greater advantages when buying other systems in future. The initial steps taken today will be built on over time, in an approach that involves migrating from today's restrictive 'closed' systems towards the business benefits achieveable with open ones.

BOOK REVIEW



TITLE:
An Audit Approach to Computers

AUTHORS:
Brian Jenkins, Peter Cooke, Peter Quest

PUBLISHER:
Accountancy Books

PRICE:
£55.00

PAGES:
572

At 572 pages, this is indeed a heavyweight book, and in more ways than one. The back cover states that 'the book will be of particular relevance to the practising accountant' and this is at once its strength and its weakness. The authors are all partners in one of the major accounting firms and the book is aimed squarely at external auditors. It deals with this area of computer audit competently enough and from that point of view alone it is likely find a home on the the bookshelves of external auditors. But what about the rest of the computer audit world?

Despite the claim that it will also form 'an excellent practical basis of work for internal auditors, I found that it barely mentioned the differences between internal computer audit and its external counterpart and this was reflected in the example systems, which are the traditional financial applications. No mention here of auditing airline reservation systems, just-in-time ordering, the efficient running of a spare parts operation, or keeping nuclear power stations from melting down. No, if it isn't P&L, or balance sheet, then it doesn't really exist as far as fee earning external auditors are concerned.

Indeed, the title should really be *An Audit Approach to Computers - Verifying the Accuracy of the Financial Statements*. If it had this title I could not quibble with its content, layout, or style. After all, accountants are meant to be boring, so one would expect a competent, but rather boring book, which is exactly what this is.

John Mitchell

Document Image Processing: The Auditor's Challenge for the 90s!

K N Tombs

I am not an auditor as you can see from the biography attached to this article. Therefore what am I doing writing an article for the *CASG Journal?* The answer is quite straightforward, but involves a little history from about ten years ago. In the early nineteen eighties I was primarily involved with facsimile and office systems, moving images of documents between businesses or government buildings. The computer industry was heavily involved with wordprocessing PPC*, and was set to promote image processing as the end for paper produced outside of the organisation with WP ending paper within.

My exposure to this embryonic and much hyped field sustained my interest as a consultant to the present day. In early 1990, I began to realise just how fundamentally important paper avoidance would be to many organisations from the projects I was involved with at the time. However, over and over again one specific issue raised its head, the issue of legality of these electronic versions of paper.

This repeated exposure to the problem lead me to start a research project into the legal and management issues of document image processing. Carried out under the watchful eye of Brighton University (née Polytechnic), this research enabled me to formally investigate the legal issues and management perceptions of I.T. and the law.

The results were to my mind quite surprising, the real management issues with document image processing were the traditional attitudes towards I.T. and changes to working practices. The repeated issue of legality was often used as a brake to adopting dip, to slow (and often inhibit) the journey into the paperless world. To be fair, paper does have strong psychological connotations apart from being a light weight low energy consuming way of taking your information with you.

So here we have a knowledge gap between management and the legal profession, one which seemed to readily generate confusion and mis-understanding. The lawyer would hedge his statements with ifs and buts and maybes, whilst the executive about to spend a million pounds on a dip system sought cast iron certainty.

The basic process of document image processing is the taking of an image copy constructed from many thousands of points of pixels. Each one of these pixels is positioned line by line across and down the page, each point being effectively a black or white point[1] on the page.

Unlike computer codes in character formats, what derives from an image system is a *bucket full of bits.* These buckets are termed *binary large object files* (BLOBs) and can be very large, even when the white space has been electronically extracted from the file. These strings of binary are extremely difficult to edit at machine code level because the compression methods use sophisticated mathematics. However, modern graphics systems have the capacity to import those strings and expand them back to a working image, making it very easy to edit these strings.

Unfortunately, these highly secure binary strings become readily edited by any DTP artist. It is exactly this ease of modification which bedevils document imaging in just the same way as conventional character based computing. This ease of modification promotes highly managed procedures around the image system to impede any unauthorised handling of images.

In the broader perspective of legally usable evidence, unlike computer generated evidence which seldom forms the only evidence for a case, documents quite often form the core of a case. Therefore, courts depend to a much larger extent on documents, and potentially their electronic similes, which in turn requires the validity of a document to be ascertained.

The only computer storage media which can meet the requirements for unalterable image and data storage is the optical disk. For all working purposes[2] the WORM optical disk cannot be modified, only destroyed, and provides as true an indelible version of a document at an instant in time as is currently possible.

The need to achieve legal validity for electronic documents is quite different to that of existing computer applications, and in the same breath quite similar. The sameness derives from the conventional database and index methods used to reference the images, the procedures to control them and how the users are managed. The difference derives from the longevity of storage required to meet the existing laws and customs based on paper files. For example, the Inland Revenue has to keep large sections of their paper (4 billion sheets!) for about a decade after the

---

* PPC, Pre Personal Computer

person has died, whilst corporate and trust materials may have to be kept in perpetuity†.

The majority of organisations have to keep (although many don't), records for decades. Health and Safety records for certain categories of staff have to be kept for life plus ten, a lot of paper to be held for a long time.

Returning to my story, to make certain, or at least to reduce the risks associated with electronic images being usable in court, a rather more pro-active approach is required. Such pro-action is not typical of many businesses and here arises the challenge; for whilst the processes of auditing and certifying computer systems before or after the legal event are well understood and practised, the need to audit management style and philosophy is an awkward proposition. This is particularly true when to most managers audit is at best a nuisance instead of the protective mechanism it is to shareholders, customers and employees alike.

We have solid historic evidence which shows just how difficult it is to audit a business, based upon accounting procedures only. Previous articles in the journal have commented on the need for a broader base of audit, one which includes qualitative judgements about business reliability or, in this context, systems viability. With image systems they require formal certification from day one with affidavits or certified statements stored on the system itself, for if called upon in twenty years time to provide evidence, I may no longer be alive to testify. In certain court cases the opposition will try every ruse to discredit your evidence, and if there is no supporting testimony to show that the system has already worked reliably, your evidential arguments may be weakened or discredited.

Here comes the challenge again, for the documentary evidence does not *exist* within the image systems itself, it exists in paper form before it is scanned and destroyed – procedures must encompass both machine and management practice. With many systems becoming available today, the document never actually exists as a single entity, but in a series of interlinked pages, spread-sheets, DP tabulations, comment notes and even voiced messages. How in the future can any auditor genuinely make the statement that the material compiled from dozens of different sources is true and valid? How can an auditor under present circumstances expand a methodology to include quantitiate and qualitative information derived from the areas surrounding the image system? How can we show or measure that some vindictive member of staff is not getting their own back on a plaintiff or defendant?

A separate but equally important aspect of audit is just how do you investigate document storage volumes in the Terrabyte[3] ranges? Just how do you search for one lost document in 200 million? Current tools for audit purposes just do not exist at present, but will be increasingly demanded during the coming decade.

I suspect that the answer will be that the courts will still rely on a qualified statement of validity, solely on the bases that documents do not prove a case on their own. Such a statement will require *intelligent* audit tools and procedures to be applied and validated.

Image processing can undoubtedly make significant impact to the bottom line of many organisations, values of 40 to 70% reductions have been quoted. Image can potentially shorten the litigation process by speeding up the compilation of court document listings. Indeed, several high court judges have stated their preference for the paperless courtroom, with a single set of optical disks holding everyone's papers correctly indexed, available in seconds.

There are many other related issues, issues such as what happens to the papers of companies going into liquidation or receivership? How do we validate chains of information sources which ultimately get stored on my dip system? How do we construct an audit methodology that can realistically measure both hard accounting and philosophical aspects of an organisation?

From my perspective, the computer audit profession has to anticipate those needs and indirectly drive the creation of supporting audit tools. In my opinion, audit method can only be successfully applied to document image systems at the optical disk level, working outwards to investigate error or omission.

To make a positive contribution towards starting this process, I would be prepared to organise a workshop on the subject if the level of interest is high enough. There are potential tools available, but these and ideas for new tools need to be formulated and promoted to developers and users alike.

Image processing is coming and will impact many organisations in the same way as accounting, manufacturing and word processing did in their turn. I would like to feel that it should be possible to anticipate the legal certification needs of image systems before the event not after it. Particularly when large organisations become totally dependent on the screen and not the paper.

† this is in itself a problem for plastic coated fax paper often lasts only a year, and modern papers may remain intact for 20 to 30 years.

BIOGRAPHY

Kenneth Tombs is a leading "independent" consultant on information systems and document image processing. During the last twenty years he has supported organisations such as British Rail, Basildon DC, Bank Of America, American Express Bank and Shell. Beginning his working life as an apprentice engineer, his most recent work includes advising corporates, the Cabinet Office – CCTA and other government departments on justifying and implementing document image systems.

1. alternatives to black and white exists through photographic type grey scales, or multiple layers of grey shades as found on x-rays and in true photographs.
2. this statement holds true unless highly specialist techniques are applied to the disk media, techniques not appropriate for public scrutiny at present.
3. Terrabyte, $10x10^{12}$ bytes. Many commercial document stores will consume optical storage at these levels and recently available CREO optical tape can store 1.3 Tbytes online!

Footnote

If anybody would like to contribute to the development of ISO and BSI DD 206 (Legal Admissibility) or is interested in a workshop on this key issue, please contact the author on 0342 832610.

EDPAA Special Interest Groups
AS/400 Security SIG

The AS/400 Security SIG is planning to organise a workshop on AS/400 Auditing and we are taking this opportunity to invite you to register your interest.

The objective of the workshop will be to discuss the various aspects of security and control of AS/400s and to produce a complete programme to facilitate audits of this complex system. Following the event all participants will receive a copy of the audit programme for their benefit.

The workshop should be an excellent opportunity to acquire knowledge of AS/400 auditing features and obtain a practical audit programme based on a pool of different auditors' knowledge and experience.

This kind of activity has been attempted very successfully by other groups such as MVS auditing and we are intending to apply a similar formula for this event.

The workshop should involve about 30 participants with at least some existing knowledge of AS/400s, not necessarily all experts in the field. EDPAA membership is not essential and we would welcome persons from any organisation who are interested in coming along and participating.

The SIG is particularly keen to hear from any organisation that would be prepared to host the workshop. The requirements are for a large conference or seminar room or perhaps a number of smaller rooms where groups can work together. The accommodation would be required for the entire day.

If you would like further information about the workshop or would like to register your interest, please contact Alan Parkes at National Australia Bank on 071-606 8070.

A New Service for Group Members

Library services for BCS members

The IEE/BCS library has been housed at the Institution of Electrical Engineers (IEE) since 1977. The entire book collection exceeds 50,000 items, and periodicals amount to over 3,000 titles.

Users of the library will find one of the largest collections of material in the fields of electrical and electronic engineering, computing, control and management. Books and journals on computing make up over 50% of the recent collection covering all areas of the subject. The areas are too numerous to list here, but a sample list includes systems analysis and design, programming and languages, operating systems, artificial intelligence, computerised control etc. as well as an extensive collection of directories, dictionaries and other reference books. CASG members will be particularly interested in the section dealing with computer security and fraud.

Since the merger in 1991 of the IEE and the Institution of Manufacturing Engineers, the library collection has been enhanced and now boasts a respectable coverage of books and periodicals in the field of production engineering.

Members of the BCS may take advantage of a range of library and information services.

(a) *Lending and Reference Services:*
Members may borrow up to six books for a period of four weeks and may renew it if the item is not required by another reader. A postal loans service is available free of charge.

(b) *Photocopy and Document Supply Services:*
Members may obtain photocopies of articles from journals and conference proceedings under the terms of the Copyright Act. Items which are not in our stock can be obtained through inter-library loan.

(c) *Technical Information Services:*
The library incorporates the Technical Information Unit (TIU). This unit has access to over 1,000 of the world's major technical and business databases and maintains an in-house marketing database. BCS members desiring market and/or technical information may discuss their requirements with trained information officers and appropriate information sources will be consulted to provide customised answers to enquiries. Estimates of cost will be given in advance.

(d) *Courses Information Services:*
The courses officer provides information on courses in higher and further education for career development and continuing education. A separate listing of courses entitled "preparing for the BCS examination" is available.

(e) The BCS librarian maintains a collection of current and archival material pertaining to BCS activities and news from the Specialist Groups.

Library and information services are available between 0900 and 1700 during the week.

Further information on a price lists for any of the services described above may be obtained from:

Ginny Bennett, BCS Librarian,
Institution of Electrical Engineers,
2 Savoy Place, London WC2R 0BL
Tel 071 240 1871 ext. 310,
Fax 071 497 3557.

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?

JOIN UP AND SAVE MONEY!

On this very page you will find below that CASG membership entitles you to a discount on the subscription price of the Quality Software Report newsletter.

This is not the only discount that we have negotiated on your behalf. As a reminder, CASG membership entitles you, in addition to the discount mentioned above:

1) £50 reduction for attendance at COMSEC 92;
2) 20% reduction in the subscription price of the *Computer Fraud and Security Bulletin;*
3) 20% reduction in the subscription price of *Computers and Security*
4) A saving of about £50 on our own Annual Conference.

As Corporate membership costs only £50, you soon realise that membership of CASG can actually save you many hundreds of pounds each year.

This is in addition to free attendance at our evening meetings, a quarterly Journal and the opportunity to take part in discussion groups. In fact, if you join CASG you actually save money and learn a lot about computer auditing at the same time!

Please mention your membership and the benefits it brings to other auditors. The larger our membership the more weight we have when negotiating on your behalf.

YET ANOTHER DISCOUNT!

We have managed to arrange a 25% discount on the *Quality Software Report* newsletter. In view of the move towards TickIT certification and the current ineterest in quality assurance, we feel sure that you will find this newsletter of interest. Why not see a copy for yourself before you make a decision? Contact Janet Wood on the number given on the order form below for more details.

PLEASE SEND ME
The Quality Software Report for the next twelve months, at the special price of £180.00 (a saving of 25%)

I enclose a cheque for £180 made payable to Profile Services (U.K.) Ltd*/

Please invoice me at the address shown *
(* delete as applicable)

Signature . . . . . .

Return to:
The Quality Software Report,
P O Box 2645, London W14 9ZD,
United Kingdom
Telephone 071 385 1848 Fax 071 385 1596

Name . . . . . .

Title . . . . . .

Mailstop . . . . . .

Company/Organisation . . . . . .

Mailing Address . . . . . .

Town . . . . . .

Post Code . . . . . .

Telephone . . . . . .

Fax . . . . . .

CASG offer

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)* £50
* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal (see over)

INDIVIDUAL MEMBERSHIP (NOT a member of the BCS) £15

INDIVIDUAL MEMBERSHIP (A MEMBER of the BCS) £10
BCS membership number: _____

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

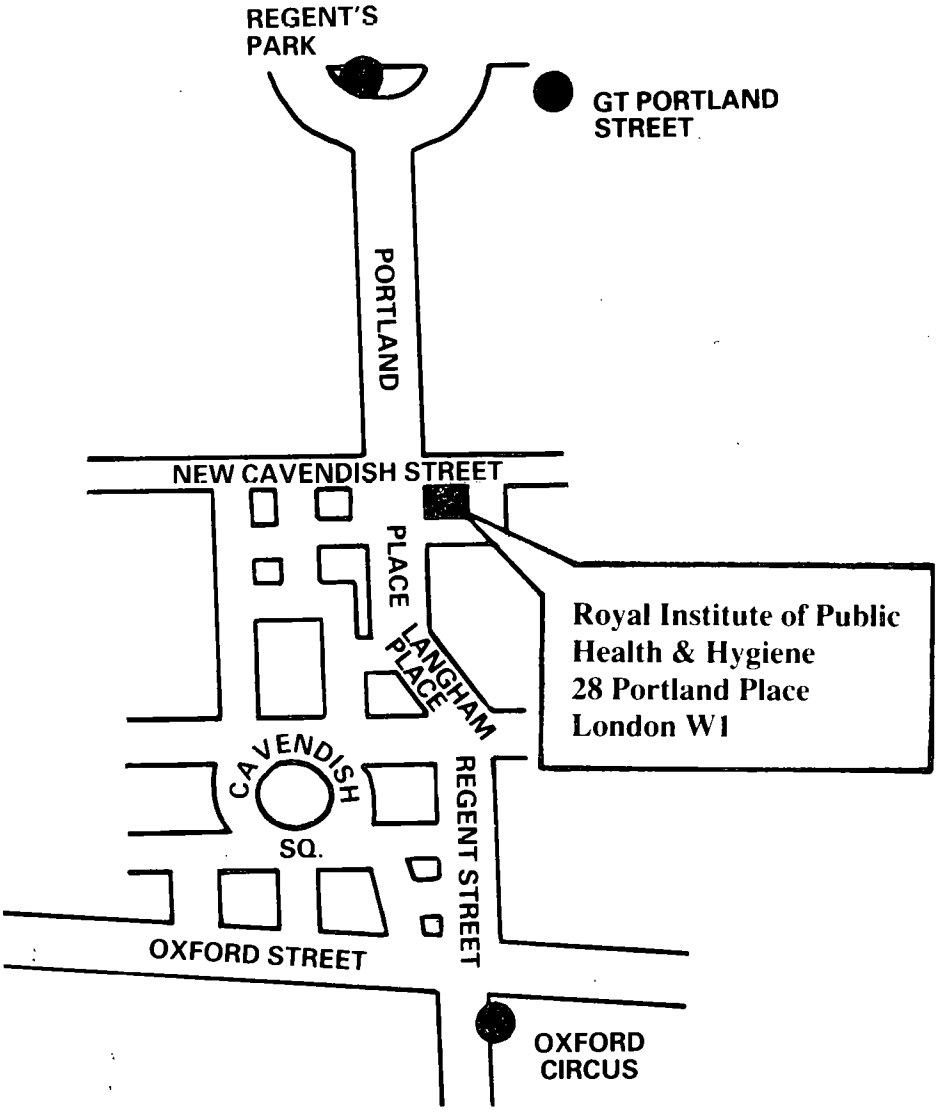
INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit   4 = Academic 2 = External Audit   5 = Other (please specify) 3 = Data Processor

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit   4 = Academic 2 = External Audit   5 = Other (please specify) 3 = Data Processor

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit   4 = Academic 2 = External Audit   5 = Other (please specify) 3 = Data Processor

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit   4 = Academic 2 = External Audit   5 = Other (please specify) 3 = Data Processor

Venue for Members' Meetings



CASG JOURNAL
SUBMISSION DEADLINES

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