IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL
volume 12 number 4 summer 2002 ISSN 0961-9348

Programme for members' meetings 2002/2003 season

Tuesday 1st October	**DATABASE SECURITY** Presenter: Alex Brewer, Lloyds TSB	Evening 16.00 for 16.30 to 18.00 KPMG
Monday 4th November	**IMPLEMENTING AND AUDITING IT GOVERNANCE** Joint Meeting with IT Faculty *Turnbull upset the apple cart by stating that organisations should consider not only their financial controls, but also their risk management processes, compliance and operation controls. This has put many IT departments on the spot as they now have to assure senior management that they have appropriate processes in place to meet these requirements. One way of achieving this is to implement an appropriate IT governance programme. This seminar examines: the concepts of IT governance; the role of risk management in the process; the importance of the control environment; where control self assessment fits in; the role of internal audit in providing objective assurance.*	Full Day Briefing 10.00 to 16.00 Chartered Accountants' Hall Moorgate Place London EC1
Tuesday 3rd December	**BS7799** Presenter: Dave Watson, Accredited Auditor *An in depth look at the interaction between a number of standards including BS 7799 / BS 15000 in a real life environment.* *This presentation aims to give up to date practical advice on issues raised.*	Evening 16.00 for 16.30 to 18.00, KPMG
Tuesday 28th January	**CYBERCRIME UNCOVERED** *TBA*	Full Day Briefing 10.00 to 16.00 Central London
Tuesday 11th February	**DIGITAL SIGNATURES** Presenter: Professor Fred Piper	Evening 16.00 for 16.30 to 18.00, KPMG
Tuesday 18th March	**SYSTEMS DEVELOPMENT & AUDITING** *TBA*	Full Day Briefing 10.00 to 16.00 Central London
Tuesday 13th May	**HACKERS** *Presenter: John Butters - The Ernst & Young Tiger Team* *An inside view of an attack and penetration squad that uses skills that go beyond normal penetration testing. As well as off-site attacks, they use techniques to gain access into computer networks which include physical entry via ceilings, stolen key cards and social engineering.*	Evening 16.00 for 16.30 to 18.00 KPMG

To be preceded by IRMA AGM

Please note that these are provisional details and are subject to change.

The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.
For venue maps see inside front cover.

Contents of the Journal

Venue for

Full Day Briefings

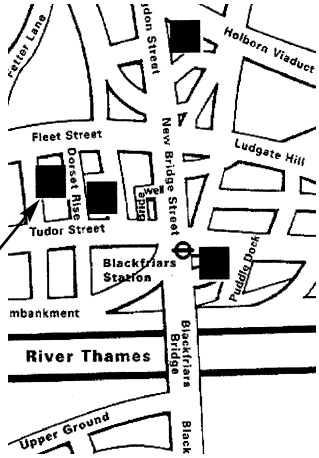
(except 4 November 2002)

Old Sessions House
Clerkenwell Green
London EC1

Venue for

Late Afternoon Meetings

KPMG
8 Salisbury Square
London EC4



The ***Journal*** is the official publication of the Information Risk Management & Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL
Email: john@lhscontrol.com

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by PostScript, Tring, Herts.

Editorial

I went along to Iinfosec 2002 for a day, partly to help out the BCS by attending their stand and promoting IRMA, but also to see what the latest security gizmos were like and to listen to a couple of the free presentations. The presentations are, of course, by the exhibitors, but by and large they were not overtly commercial, were professionally done and made some very good security points. I used the opportunity to collar a couple of speakers to write articles for this Journal and they will be appearing in due course. My *modus operandus* is simple and follows my 'unsafe' audit approach. "What's this all about", I hear you squeal. "Mitchell's having another of his philosophical attacks. Time to skip to the rest of the Journal". Well, you may be right, but bear with me a little.

There are only two types of auditing in all of the observable universe and neither of them are taught by the IIA, or the universities, so it must be worth reading on. The two types are 'safe auditing' and 'unsafe auditing'. The former is done by most auditors. I think it forms part of the curriculum. Safe auditing is when you go into your office in the morning, shut the door behind you, lock it and put the back of a chair under the handle so that no-one, but no-one can get in. You then log into your workstation, prepare reports that are more beautiful than an illuminated text, cross-reference your working papers to an extent that you will earn gold stars from your external auditors, you try to talk to people on the telephone, who are seldom available, who never return your calls and if you are lucky enough to get them you find that mysteriously they cannot hear your questions. Your reports are beautiful, but full of self-evident trivialities. That is safe auditing.

Unsafe auditing is when you take the chair from beneath the door handle, unlock the door, open it and start prowling around. It is decidedly unsafe and dangerous. Walk against the side of the corridor with your back turned slightly towards the wall to protect you from that knife. Beware of the garlic smelling, crucifix holding humans who you come across, who a few seconds after seeing you will attempt to flee. Lurk by coffee machines. Keep completely still and after a time no one will notice that you are there. They will say the most damaging things without knowing that these are being recorded by you. Take a deep breath and enter the smoking room. Listen intently and then, just as you are about to pass out from oxygen starvation, leave and write up your notes. Go to the canteen, pretend to be absorbed in a book on 'how to make friends and influence people', as you twiddle with your food, while all the time listening to people sending themselves to eternal damnation. Sit in the toilet cubicle with your feet off the ground and listen to the idle chatter of people as they wander in and out. Another five pages of notes. Disguise yourself as a human and when you see that person you have been trying to interview for months walking towards you, ask them whatever killer questions you have been storing up. They are ill prepared, out of their normal environment and are vulnerable. They don't have time to think up a plausible explanation for their misdemeanour and answer truthfully. You scuttle away and write up your contemporaneous interview notes as you go. This is unsafe and dangerous auditing, but what an adrenaline rush. You get results!

So now you know how I find my contributors, Not by sitting in my office, not by telephone, but by hunting! So at the next meeting, when you see a smiling Mitchell approaching you and you realise that you have left your defences at home, don't fight it, succumb with due grace, it won't be as horrible as you think. Just say 'yes' to that question "will you write a little article for me?". Join the band of the un-dead. Live a little!

Which brings me to this edition's contributors. Lee Ann Kalaba discusses the benefits of CAATs in the audit process and gives examples of their uses. Raymond Wessmiller deals with the issue of data integrity and provides a case study as to how co-operation

Editorial continued

between the financial and computer audit teams shaped an entire audit. Paul Golding provides an update on data and the law. Our secretary, Siobhan Tracey, deals with business continuity planning whilst our resident events reporter, Rupert Kendrick, provides a write up on our last full day event which dealt with that very subject. Andrew Hawker, our spiderman of the web, deals with the deadly sin of 'ultracrepidation', or does he? There are the minutes of the AGM which are supported by the Chairman's report and an update on our financial situation from Mike Demetriou our retiring Treasurer. Colin Thompson, the BCS Deputy Chief Executive, provides his usual full account of what's happening to our parent body. Finally, there is a bumper humour section to see you through the Summer break.

No break for your committee however; we will be working hard to create next season's programme. Which reminds me ……. subscriptions are now due and you should find a renewal notice amongst the various advertising flyers.

You may know this already, but previous editions of the Journal can be found on our web site (www.bcs-irma.org), along with a host of other useful information and links.

Happy reading and I look forward to seeing many of you at our meetings next season..

John Mitchell

Chairman's Corner

John Bevan

The May 14th AGM marked the end of one IRMA season and the start of another. We welcome a new Treasurer and Secretary, but still have the same Chairman. Despite my being inactive for most of last season, for family reasons, I was re-elected. Why? There were no other candidates. However I feel that it is time for a change, because I have been Chairman for a few years, and because I have not been active in risk management or audit of late. I hope that one or more suitable candidates may emerge over the next year so that at the next AGM you may choose a new Chairman. The group ought to have a chairman who is active in risk management, information security, and audit, but this relies upon members coming forward to support their specialist group. Last season we re-introduced a buffet at the end of the late afternoon meetings, so that members could "network", meet committee members, and generally feel more involved in the group. I hope that we can improve member participation in the group this coming season, in this and perhaps other ways.

If you look at the Chairman's and Treasurer's reports for last year you will see that although we experienced an increase in membership, we continued to run at an operating loss. Our asset position remains healthy however. Your management committee is not complacent about this position, and is shortly to carry out a thoroughgoing review of all of our activities, membership, costs, fee income, etc. If you feel that you would like to contribute to this debate, then let me know your views as soon as possible.

One change we are considering is the greater use of e-mail to communicate with members. We would hope that this would not only reduce costs, but also introduce more flexibility in communicating with members. You may have noticed that I sent a letter about BS 15000 to all members dated April 10th. It was delayed by its inclusion in the bulk end-of-April mailing to all members. With e-mail this need not have happened. We might also use e-mail to communicate more selectively with some members, for example over a topical issue affecting mainly bankers, or to postpone a meeting scheduled for a day when a transport strike was likely. Whatever we decide to do will first require that we have new admin systems in place, as well as the approval of individual members. After all I suspect that not all members will want or even be able to receive IRMA news by e-mail!

In response to my recent appeal for help in reviewing revisions to the BS 15000 standard (on IT Service Management), I was very pleased to receive some twelve offers of help from members. We hope to review the next draft, and to submit our comments to the British Standards Institution via the BCS Security Panel. IRMA only occasionally does this sort of work, but it may be an example of an increasingly important and pro-active role for us. I am not yet sure when this will take place, but I shall keep you informed on progress.

Are you aware of BS 15000? Much to my surprise most of the speakers at last year's outsourcing briefing were not. If you need to review an outsourcing or service level agreement then you should look at it. Your IT people should also be aware of it. See the BSI web site www.bsi-global.com and search on "15000" for more information.

Facing the Data Integrity Challenge

By Raymond Wessmiller

Many auditors do not want any part of testing the validity and reliability of data from computer files. Many don't perceive testing to be directly related to their audit objectives. Others think it will take too long. Still others believe testing will require them to have special skills and knowledge and master complicated audit software.

A change in attitude is called for because many easy-to-use audit tools are available to help auditors meet the data integrity challenge head on. Verifying the integrity of data before proceeding with audit objectives is essential because auditors must ensure the conclusions in their reports are based on accurate and reliable data.

The premise auditors should start with is: "Is the data reliable enough to meet my audit objectives?" Historically, computer evidence has been treated as being unique, but it is really no different from any other audit evidence and needs to be verified. For example, the U.S. Government Auditing Standards yellow book states that government auditors must obtain "sufficient, competent, and relevant evidence" that data is valid and reliable if their report conclusions, recommendations, or findings depend on computer-generated data.

When verifying data integrity, government auditors have three choices:

- Rely on the work of others who established the validity and reliability of the data.
- Perform direct tests on the data.
- Test the effectiveness of general and application controls over the system that generated the data.

Most often, auditors consider only the third option, and then quickly decide they do not have the technical resources or time to test general and application controls. In the end, they issue their report, never mentioning data integrity, or at best, they bury a disclaimer in the small print of the objectives, scope, and methodology section.

Not surprisingly, where government computer systems are involved, it is likely that the source data is not reliable. The evidence is overwhelming that federal agencies have major problems in designing, implementing, and operating computer systems. If you are not convinced, consider the fact that just during the last 12 months or so, the General Accounting Office has issued about 250 reports that highlight significant problems related to federal computer systems. The predictable outcome of these problems is that many systems maintained by federal agencies probably contain unreliable data.

What good is an audit report that has conclusions, recommendations, and findings that might be based on faulty data? Audit software tools make it easier for auditors to verify their data and produce more reliable audit reports.

A Cautionary Tale

Let me share a recent story from the audit trenches that shows what can happen when auditors test data validity and reliability. One of my jobs at the GAO is to help ensure that auditors follow appropriate methodologies in planning their audits – including compliance with yellow book section 6.62 on data standards. One particular assignment called for the audit team to determine whether publications maintained and sold by an agency (the name doesn't matter) were available only within that agency, or were available elsewhere, including Web sites such as Barnes&Noble.com or FirstGov.gov.

For this assignment, the audit team planned to select a random sample of publications from a database that, according to the agency, contained information about all publications maintained by the agency, such as publication name, date, price, author, and cost. Using Internet search engines, the auditors then planned to see if the items selected in their sample were also available at various Web sites. At the end of it all, they planned to project the results of their sample and issue a report that concluded with something like: "Seventy percent of publications maintained by agency X are also available on public web sites." At the point our data reliability team intervened, the audit team was ready to select a sample, but they did not know what sample size to use or how to obtain a copy of the database and actually select the items for testing. One of the first questions we asked was: "Do we know that the information about publications in the agency database is complete, current, and accurate?" We got the same response I usually get from students in the training classes I teach – silence. We knew the auditors did not want to address this question, but we informed them it was essential to first verify the integrity of the data before they proceeded with the audit objectives.

The first step we recommended was to interview agency officials to determine if there had been any material or adverse findings relating to the functionality of the system that contained the data relating to publications. We advised them to consider reports issued by the Office of Inspector General, Chief Information Office, Chief Financial Office, or any other internal audit group. If there have been any adverse findings, we asked them to obtain copies of the audit reports and determine if the findings could affect the integrity of the databases created in response to our request.

The next steps were to: Identify the data elements deemed critical to the audit objective, such as publication name, date, and author. Request a data file of all records with these data elements. Randomly select a sample of publications from the file and trace them back to the source publications to verify that the publication name, date, and author were correctly recorded in the database. Since the agency said that all publications it maintained were stored in one physical warehouse, the approach seemed simple and straightforward. Here is the sequence of problems and discoveries as they actually happened.

Records Missing From the Database

After we examined the data element dictionary for the system that contained information about all publications (which I'll hereafter refer to as the PUB.SYS), we requested a data file containing all records and the critical elements we needed to verify. The first response from the agency was that the file would be too big to process on our microcomputers. They defined "too big" as "somewhere between 3.5 and 4.0 million publications." When we told them we had experience with files as large as 45 million records (12GB), they relented and quickly provided a 400MB file on CD-ROM. We proceeded to import the file into our audit software, IDEA, and soon noticed there were only 2.3 million records. What happened to the other half? When we inquired at the agency, they seemed almost as surprised as we were. But, after checking with some employees who had been

with the agency for many years, they discovered that about 1.2 million publications had never been entered into the PUB.SYS. These publications we learned, were catalogued on 3-by-5-inch index cards maintained in a library-like manner within a room of the warehouse. Should we have included these publications as part of our integrity test? The answer was an unequivocal yes because the audit objective was to determine if all publications maintained by the agency were available elsewhere. Nobody said the documents had to be stored in a database. So, the auditors learned that in addition to verifying database integrity, they had to design a test to verify the integrity of the card system as well. To do this in a statistically valid manner, we recommended the following steps:

Count the total number of drawers (900) that contained index cards and label each drawer one to 900. Generate a set of 75 random numbers between zero and 901 to select 75 drawers at random. Measure the length of all cards within a drawer from front to back (15 inches). For each of the 75 drawers, generate a set of random numbers between zero and 16 inches to identify a random inch. Count the number of cards within each inch (130). Generate a random number between zero and 131 to identify the card to select for detailed testing.

In summary, the audit team randomly selected 75 cards from 75 randomly selected drawers to trace back to the source publications.

Duplicates, Blank Records, and Illogical Parameters

With the entire database in IDEA, it was easy to perform generalized integrity tests such as a check for duplicates and blank records. Within minutes, we discovered that for one of the key fields – "accession code," a unique code that enabled the agency to physically locate a document – there were 20 blank records and another 38,499 where the same entry occurred more than once. Combined, these irregularities comprised about 1.7 percent of the total number of records in the file. This may not be an alarming percentage, but it is a sign of possible data integrity problems because it indicates the system lacked basic front-end data entry edits. Additional generalized testing revealed more anomalies. For example, in a key date field – year of publication – there were 9,824 blank records, 46 with a value of "00," and about 150 records that contained unexpected dates such as the value "4" and "2018." The dates in all other records ranged from 1899 to 2000. In the month field, 502,463 records were blank (about 22 percent of the total number of records) and another 414 records had odd month names, such as "Pat" and "Fie." These discoveries pointed to more serious data integrity problems.

Documents Not Maintained by the Client

Randomly selecting items from the database was simple using IDEA software. We selected "Sampling/Random Selection" from the menu bar and completed the dialogue boxes. When we went to the warehouse to locate the publications, a problem developed – two of the documents could not be located. We met with agency officials to discuss this finding and soon learned that certain categories of publications, which fortunately could be identified in the database, were not maintained by the agency we were auditing, but were instead maintained by another agency. Based on this discovery, we decided to purge the database of some 100,000 publications that were not stored by the agency and select a second sample. At this point, the auditors had still not approached their audit objective; they were still in the data integrity-testing phase.

Your initial reaction to our discovery of this problem might be similar to mine: "Why didn't the agency tell us about these categories before we selected the sample?" The truth is the agency did not know until we informed them. The agency had been storing documents in one database or another since the 1950s and over time the audit trail had been lost. This is what happens with computer systems. People responsible for systems come and go, system documentation is often weak, bad data is migrated from a legacy system to a new system, and based on a little integrity testing, auditors will find the data is not complete, current, and accurate.

An Incomplete Database

Completeness – ensuring everything that should be in the system is, in fact, in the system – is often ignored in data integrity testing. To ensure that the data in the PUB.SYS was complete, we designed another test. When we visited the warehouse to locate and collect the publications in our sample to trace from the database, we randomly selected another sample of publications from the warehouse to trace from the warehouse back to the database. We selected these publications by randomly selecting a publication that was stored in the warehouse to the left, right, above, or below the publications selected for the sample items in the first part of our test. Again, using IDEA, we performed a match with the second sample of publications against the PUB.SYS. Not surprisingly, five of the publications stored in the warehouse were not recorded in the database. This added another data integrity problem to the list.

Considering all the problems noted above, any audit team would likely conclude that the PUB.SYS did not contain complete, current, and accurate information. Their audit report would include this finding and recommend that the agency take corrective action.

Help is on the Way

Additional help in meeting the data integrity challenge will soon be available in the form of a new publication to be issued by the GAO, Computer-Processed Data: Assessing Reliability for GAO Use. As a supplement to the yellow book, this guide provides a framework for assessing the reliability of computer-generated data and identifies some common sense and more sophisticated tests that auditors can perform to verify data integrity. The guide also explains the steps in a final assessment and the actions to take depending on the results of additional work. Finally, the guide provides suggested language for reporting the results of the assessment.

The events related in the story from the audit trenches and the availability of audit tools and the new GAO guide should leave auditors with a clear message. If their audit findings, conclusions, or recommendations are based on computer-generated data, they should meet the data integrity challenge head on and first ensure that the data is valid and reliable.

For information on the GAO guide, contact
Barbara Johnson at Johnsonb@gao.gov
or Ray Wessmiller at wessmillerr@gao.gov.

Raymond Wessmiller is a Senior Computer Specialist in the U.S. General Accounting Office. He has 20 years of experience as an IT auditor and has been an instructor and guest lecturer on using CAATS to test computer files at the GAO for the past eight years. He is a past chapter president of the NCAC/ISACA.

This article is republished, with permission, from May 15, 2002 issue of ITAudit Forum (http://www.theiia.org/ITAudit).

Preparation for Information Systems Disaster Recovery Plans

Siobhan Tracey

In the Information Age most companies have become heavily dependent upon their computer systems. It is vital for their continued existence that contingency plans are developed, to ensure continuity of operation in the event of a man-made or natural disaster. Information System Disaster Recovery Planning is an integral part of any business continuity plan and general computer system operation. It should be a dynamic process that changes as the computer environment changes.

In order to create a disaster recovery (DR) plan it is necessary to be clear about what you want to achieve from the plan and when the plan needs to be activated.

The disaster recovery planning process consists of four stages:

- Development and documentation of the plan
- Testing the plan to identify weaknesses in the plan and to ensure that the key objectives of the plan can be actioned effectively
- Review of the plan in the light of the testing results and whenever the computer operations or priorities change and
- The development of tasks/steps required to bring the computer operations back to standard operation once the reason for the disaster is resolved.

This paper deals only with the development and documentation of the plan.

As with all plans, the DR plan requires:-

- to be sufficiently detailed to cover all aspects of the computer operation, both software and hardware,
- to be fully tested and kept up to date to reflect changes when they occur. The updating of the plan is best served if it is an integral part of the change management process.
- It is important that the business as a whole is involved in the creation of the DR plan otherwise it will be seen as an Information System department initative and of no importance to the rest of the business.
- it must have senior management support, if the plan to be accepted and successful.
- the responsibility for the maintenance and testing of the plan needs to be clearly stated and enforced.

So how do we go about the development and documentation of the plan? I have set out a series of steps, which I believe are necessary for the preparation of DR plans, irrespective of the size of the company.

Step 1.
Identify the Mission Critical IS systems within the organisation:

These are the systems for which the company is dependent upon for it's successful operation.

1.1 Identify and list all IS equipment and the applications/systems run on it, (hardware: PC's, mainframes, Unix boxes etc. software: packages, in-house developments, customised software, etc.). The easiest way to do this is to list all the hardware, including its configuration and all the software in use on that hardware.

Table A is for the listing of all **Hardware**

XYZ Plc Disaster Recovery Checklist					
Listing of all hardware		Location:			
Name	Make	Model	Serial Number	Location	Location Code

Table B a template for the **Hardware Configuration**

XYZ Plc Disaster Recovery Checklist					
Listing of all hardware		Location:			
Name	Make	Model	Serial Number	Location	Location Code

Table C is for the listing of **Software**

XYZ Plc Disaster Recovery Checklist			
Listing of all software			
Machine Name	Software held on machine	Software Specifications	Licence String held

Most organisations will have a listing of their software and hardware, these need to be checked to ensure that they are comprehensive and up to-date.

1.2 Establish which systems/applications are critical to the operation of the business (e.g. sales order processing, stock control, computerised weighing scales, purchase ledger). The IS department should not decide which applications are business critical without the involvement of the other business areas.

1.3 Establish which data files are associated with the critical systems and are deemed critical by the business. Make

sure that up to-date copies of these files are held, (e.g. product price files/databases etc).

1.4 Prioritise the applications/systems in order of importance to the business. The recommended priority rating is the high, medium, or low classification given to the system in a disaster situation where:

High = required within xx hours (eg 2- 24hrs)

Medium = required within xx hours (eg 72hrs)

Low = required when available

Remember the longer the delay in restoring the system the greater the impact on the users and the business.

1.5 To perform 1.2, 1.3 and 1.4 above, it is necessary to establish the maximum time allowable for the repair of any breakdown in these systems/applications. This is generally the length of time that a user is able to carry out the business function before requiring computer access.

1.6 Remember the criticality of the application can be dependent upon the time/day of the week when the disaster/major problem occurs; eg payroll may be low priority on Monday but a high priority on payroll processing days.

Step 2. Ensure there are Adequate and Appropriate Back-up and Recovery Procedures

No recovery can be actioned if there are not the correct data to recover. The business generally takes back-up of its systems on a regular basis. However if the back-up cannot be recovered then the back-up only provide a false sense of security to the business.

2.1 Ensure that copies of all systems/applications program code/system disks and critical data are held in a secure and safe location, preferably off-site. It is vital that they can be easily retrieved in case of emergency (e.g a bank safe is impossible to access outside of banking hours). It is important to have a list of these files together with the file's name and contents and where the files are held (ie. their location(s)).

2.2 Ensure that the copies of all systems/applications code/programs held off-site/secure location are those currently in use, (e.g. latest version of the package etc.)

2.3 In the case of UNIX based systems, the current system configuration should also be held off-site to enable the rebuilding of the UNIX box to the same specifications.

The methodology used to restart the system, as well as how to restore to normal running should be established, verified and fully documented. This should include all interfaces and dependencies. The recovery and restart procedures for the systems should be available for all the necessary files.

Step 3. Is the location where the data is held secure

3.1 The use of secure/off-site storage must be comprehensive to enable access to the systems/applications, system data, system documentation and records. The secure/off-site storage should ensure that the critical computer systems back-up filed can be FULLY restored with minimum losses being incurred and consistent at a point in time. It also needs to be consistent with files held at alternative sites, which may or may not be affected by the disaster. This is particularly important to-day with wide scale application integration. The secure/off-site storage does not necessarily have to be at one location.

3.2 Data held in a secure/off-site location should include:

3.2.1 copy of the disaster recovery plan

3.2.2 the callout personnel list, this lists who are to be called out in the event of a disaster, together with their out of hours contact telephone number(s). The list should also indicate their responsibilities. See Table D

3.2.3 copy of all applications/systems programmes

3.2.4 copy of all applications/system data, daily back-ups, if possible, otherwise at least weekly

3.2.5 copies of all system documentation, including application licences where the software is purchased as a licence

3.2.6 copies of all user manuals and associated procedures, including the way each business system will operate in disaster mode

3.2.7 all PC based data used in the management of the business eg copies of spreadsheets, databases standard documents etc.

3.2.8 A separate copy of PC software packages licence numbers to enable their replacement where necessary and to facilitate with help desk queries

3.2.9 copy of all information system related agreements, including maintenance and service contracts with third parties.

3.2.10 copy of any insurance contract together with the insurance agency contact name and telephone number.

The backed up data should be sufficient to enable a full recovery to be undertaken with the minimum of disruptions.

Step 4. Where there are Third Party Agreements (Facility Management etc)

4.1 Third party service agreements should be considered for the maintenance of the disaster recovery plan. This could enable the provision of equipment, software etc. within an appropriate time scale. Some computer manufacturers have the facilities to provide replacement machines while the computer software companies will provide the currently used version of their software.

4.2 Where an alternative site/equipment is available the practicalities of transferring operations to the alternative should be considered carefully. This includes checking the adequacy of power sources, communication facilities and office space. The plan should outline the methodology to be used to bring the alternative site/equipment into operational status.

Step 5. Communications

5.1 Clear communication paths should be defined. Since rapid communications of the problem enables quick response and appropriate actions to be taken. It is

important that a listing of all persons to contact in the case of a disaster is maintained. This list should provide contact names and telephone numbers.

Table D is the **Contacts List**

XYZ Plc Disaster Recovery Checklist					
List of Employee / Supplier Contacts					
Priority	Name	Job Title	Home Telephone	Mobile Number	Application Expertise

5.2 Clearly defined escalation criteria and communication paths for IS problems can often prevent serious problems becoming total disasters. All those involved in the disaster recovery plan should be aware of their role and responsibilities throughout its implementation.

5.3 It is important to have a checklist of those to be contacted and where/when to contact them, and that copies of the list are held by two senior executives/directors.

5.4 The communications should also include the suppliers of services and any third party involved in the actioning of the plan.

5.5 The setting up of clear lines of communications and time tables for actions can ensure that the DR team can get on and do it with the minimum of interruption from the business while people try to find out what is happening.

Step 6. User Involvement

6.1 The development of the disaster recovery plan should be undertaken with the involvement of the system users. This will ensure that users are aware of the plan and what the impact of a disaster will have on their ways of working.

6.2 User involvement at the planning stage should minimises confusion as to what IS services will be provided and the alternative procedures being operated in a disaster situation.

6.3 The inclusion of the user will ensure that

a) the actual operation of the business is reflected in the plan,

b) the users are aware of the impact of the disaster on normal activities even if they are not directly effected by the problem and

c) the users take ownership of those aspects of the plan affecting their usage of the system should the disaster plan ever have to be implemented.

Step 7. Return to Normal Operations

Consideration has to be given to how the system(s) will be restored to normal running when the immediate disaster situation is resolved. There is a need for plans/instruction for the restoration of normal activities and for the input of data ignored during the crisis.

Finally

It is important that the business understands that unless we have contingency plans for the business as a whole, the business might as well whistle in the wind, it no good having great IS DR plans if the rest of the business cannot operate. An IS DR plan in isolation is just a piece of paper with little or limited value, however when it is integrated into the Business Continuity Plan it becomes a vital tool in the process to enable a business to recover from man-made or natural disasters.

Remember the first attempt at the plan will very often result in the many questions over the processes and procedures in operation. It will also identify any gaps in knowledge with respect to the operation of the information systems. These issues should not stop the plan being developed. The DR plan needs to be regularly tested to ensure it will work and that any weaknesses in the plan are identified and corrected. Also the testing of the plan enables the DR team to become familiar with it and it's operation.

Table E Disaster Check List

Here is a listing of the normal information required when a disaster situation arises:

- System Description
- System Operations Manuals (how to operate the system)
- User Contacts for the application
- System/Transaction Priority
- Data Preparation Instruction
- System Schedule: This is a definition of when the system is run during the week or period.
- System Flow Chart: This is a chart of the flow of data through the various processing functions within the system
- System Dependencies: This is a statement of systems or files which must be run before this system
- Job Descriptions: This is a description of each job run in the computer system
- User Calendar: This is the statement of the times when the user either inputs data or can expect output from the computer system.
- Program details: These are records in terms of memory, disc usage, tape usage etc.
- File Back-up: This is recorded as part of the normal back-up and recovery procedures
- Recovery Process. These are the steps to be taken to return to normal operations.

Data and the law

Paul Golding

The law relating to information covers an extremely broad area. Apart from the obvious issues of data protection I have decided to look at some evidential issues arising out of the movement towards a paperless office, the criminal law establishing information technology related offences, current topical issues concerning the legality of the interception by employers of employee communications and certain intellectual property developments before reviewing, very briefly, the implementation of the e-commerce Directive into English law and a couple of tax developments (which I promise will be extremely brief as I certainly do not profess to be a tax lawyer!).

Data Protection

The first step to securing overall compliance with data protection legislation is for organisations to conduct an information audit. Such an audit must identify what information you have; what you use it for and, equally importantly, what you might want to use it for at some point in the future; where you get the information from and who you disclose it to (albeit identifying in general terms the types of information sources and the classes of recipient); who holds data on your behalf and in which countries information is held. The Information Commissioner has relatively recently issued some guidance on conducting a data protection compliance audit and details can be found on her website. For many organisations the depth of the guidance may appear excessive but it acts as a useful reference point.

All organisations should appoint a suitably senior Data Protection Compliance Officer with responsibility for ensuring compliance. Importantly this individual must have the requisite authority to command sufficient attention from those parts of the organisation most affected by data protection such as personnel and marketing.

As an integral part of the audit the organisation should also look to develop a corporate compliance/guidance manual. The purpose of such a manual is to allow a discussion to take place within the organisation so that issues can be addressed and a policy appropriate to the organisation formulated. A secondary purpose of the manual is to facilitate the education of employees so that even if they are not aware of the details of what is required they at least have a useful reference point, some idea of when issues are likely to arise and when further guidance is required.

Securing adequate Usage Rights

All organisations need to be sure that when they obtain personal information they secure sufficiently broad rights. One of the fundamental tenets of the Act is that processing must be both fair and lawful. However, there are other more specific conditions laid down, one or more of which must be fulfilled. One of these conditions is data subject consent but an interesting alternative is processing in pursuance of the legitimate interests of the data controller provided that such processing does not prejudice the legitimate rights or freedoms of the data subject. Interestingly, the Information Commissioner interprets what amounts to consent quite narrowly. In particular, consent cannot be inferred from a failure by the data subject to respond.

Most of us will be familiar with an application form containing an opt-out box. According to the guidance issued by the Information Commissioner the submission by a data subject of an application form with the opt-out box not ticked will not amount to consent but rather may go some way to signifying that the legitimate interests condition has been satisfied. Although the legitimate interests condition was inserted into the legislation at a relatively late stage at the behest of the direct marketing community, the Information Commissioner nevertheless seems to take a rather unexpected but nevertheless quite welcome broad and common sense view of what constitutes "legitimate interests".

I mentioned earlier the general requirement for fairness and lawfulness. Fairness also embodies the concept of the data subjects "legitimate expectation" of what the data controller will do with the personal information in question. Lawfulness is largely self-explanatory but two points are perhaps worthy of mention. Of relevance, particularly for public sector organisations, is that it must be shown that data use is within the limits of the organisation's legal powers. Public sector bodies have a particular problem with disclosing or sharing data. In this respect the Performance and Innovation Unit of the Cabinet Office have very recently published a consultation paper which proposes that data sharing within the public sector should be permitted and encouraged subject to adequate safeguards and greater transparency.

Lawfulness also requires that any use of data must be consistent with the European Convention on Human Rights which is now incorporated into English law by virtue of the Human Rights Act 1998.

Another requirement of the fair and lawful processing principle is that all data subjects must have what is called a fair processing notice provided to them or made "readily available" at the time when the data controller first processes data relating to that data subject. The notice must specify the identity of the data controller and the purpose or purposes for which the data is to be processed. The notice must also contain any (unspecified) further information required to render the processing fair according to the circumstances. As a result, such notices are commonly incorporated into regular communications with data subjects as a matter of standard practice.

Direct Marketing and Unsolicited E-mails

Section 11 of the Data Protection Act provides all data subjects with an express right to prevent processing for the purposes of direct marketing. This term is defined as "the communication (by whatever means) or of any advertising or marketing material directed to particular individuals". This right can be exercised by a data subject, by notice in writing, to the data controller at any time. There is currently some debate about the precise state of the law in the UK regarding unsolicited e-mails. Article 7 of the e-commerce Directive, which should have been incorporated into English law by now, provides that senders of unsolicited e-mails must respect public opt-out registers such as the e-mail preference service operated by the Direct Marketing Association. The UK Government decided not

to directly replicate Article 7 in the UK Implementing Regulations because it considered existing protections to be adequate. However, the law on this subject is likely to develop further in the future. There has been a considerable debate throughout Europe as to whether individuals should be required to "opt-in" to direct marketing or whether an "opt-out" regime is sufficient. On 28 January 2002 a proposal was issued for a Directive concerning the processing of personal data and the protection of privacy in electronic communications. That proposal is a considerable way from being made law. The proposal suggests that in certain circumstances prior explicit consent of the recipient should be obtained before communications are addressed to them. However where a company makes use of details obtained from an on-going customer relationship for the purposes of offering similar products or services as those originally purchased, the suggestion is that this marketing should be permitted, without the need to opt-in.

All unsolicited e-mails under the e-commerce Directive must be clearly identifiable as such so as to ensure that, if desired, they can be automatically filtered and a recipient does not need to read them if they do not wish to.

Overseas Transfers

The UK's data protection legislation reflects a European wide initiative to provide a single comprehensive regime affording individuals the same level of protection throughout the European Economic Area. As such information is permitted to flow freely within the EEA's borders However, it was recognised that these protections could be circumvented if data controllers were able to process information outside the jurisdiction. As a result the new legislation prohibits transfers outside the European Economic Area unless there is adequate protection in the receiving territory. To date, very few countries (including Hungary and certain Canadian provinces) have been approved as having equivalent legal protection. One country which most certainly did not have such protection was the United States where the concept of data protection was particularly alien and companies were regarded as being free to make use of personal information as they thought fit, subject to compliance with the general law. This conflict led to political discussions at a very high level as the impasse potentially threatened trade between the US and Europe. By way of a compromise, the so called US Safe Harbour Privacy Principles were adopted. Under these principles US businesses can elect to abide by the safe harbour principles. A company has to publicly certify that this is what it is doing and agree to abide by principles which are broadly equivalent to those under the European Data Protection legislation. To date this mechanism has not proved popular or successful. Towards the end of 2001 only a 100 or so businesses had adopted the principles primarily, I suspect, due to the fact that data protection in the European Community has not been seen to have a major impact on US businesses. Whether that changes in the future will depend upon the actions taken by the UK's Information Commissioner and her European counterparts.

Some businesses may elect to adopt an alternative option. The Act provides that overseas transfers can be made, provided that they are made subject to certain contractual terms approved by the authorities. With this in mind the European Union has published certain model contract terms for use when transferring data overseas whether to a data processor or another data controller. These terms are not particularly user friendly but they do present a relatively simple mechanism under which transfers can take place.

Security

The seventh data protection principle requires that all data controllers put in place appropriate technical and organisational measures to safeguard personal data against unauthorised or unlawful processing or disclosure. Keeping personal data secure means guarding against unauthorised access to, alteration, disclosure or destruction and accidental loss or destruction of data.

It should be noted that the legislation expressly refers to both technical and organisational measures. The latter is a reference to more procedural, non-technical measures such as the introduction of Codes of Practice (contractually binding on employees) governing the use of IT and communications systems as well as adequate building security, CCTV and the like. In deciding what is appropriate at any given time, regard can be had to the current state of technology, the cost of implementing that technology, the nature of the data involved and the resulting harm which might be caused from unauthorised disclosure or adaptation. Given the reference to the state of technology it is clear that data controllers must review these security measures from time to time if they are to comply with the principle.

The Act expressly provides that data controllers are under a general obligation to take reasonable steps to ensure the reliability of employees with access to personal data. Hopefully this is something which organisations do in any event although it is difficult to see, beyond the taking of appropriate references and checking with the Criminal Records Bureau, how reliability can be ensured.

One point worth noting is that when organisations receive a subject access request from somebody who purports to be the data subject, care must be taken to ensure that the applicant is genuinely who they claim to be. It would clearly be extremely serious if, in responding to a subject access request, information was supplied to a third party. In reality data controllers will probably only be required to make specific enquiries to check identity if there is any particular cause for suspicion from the surrounding circumstances. For example, if the subject access request spells a name incorrectly or appears to come from an incorrect address then some further enquiries might be required.

Processing by Third Parties

The Data Protection Act requires that data controllers must select data processors who provide sufficient guarantees regarding both technical and organisational security measures which they will implement. In addition the data controller must take reasonable steps from time to time to ensure that such measures are complied with. In reality I suspect that most data controllers will do very little to ensure that such measures are complied with relying instead upon their contractual undertakings. However, requiring the data processor to provide written information on security measures from time to time may be appropriate in certain circumstances. Information security is likely to be simply one factor to take into account when selecting a data processor. It would be unrealistic to expect information security to be given anything like the degree of importance given to, for example, price. However, most data controllers will at least want to be able to demonstrate that they did make appropriate enquiries as part of the appointment process. In this respect it should be borne in mind that the term "processing" is extremely widely defined and includes those who merely hold data on behalf of another organisation.

All data controllers must have written contracts with their data processors. Those contracts must require the data processors only to act on the instructions of the data controller and to comply with equivalent security obligations as those imposed under the Act on the data controller.

Formation of Contracts

Under English law, subject to certain very limited exceptions, such as the sale of land, it has always been perfectly possible to create valid and binding contracts by electronic means of communication such as e-mail. To illustrate the point the recent US decision of Shattuck against Klotzback confirmed that an exchange of e-mails had contained all the necessary ingredients to form a binding contract.

Although a number of studies have confirmed the fact that under English law there are a large number of legislative provisions which require written (hard copy) documentation, there is no generally applicable requirement. Equally there are individual instances where a physical signature is required. Again, there is no generally applicably requirement for a physical signature. Nevertheless whilst the English legal position was not particularly problematic for the vast majority of electronic transactions the legal position varied considerably across the European Community. With that in mind the European authorities passed legislation designed to place electronic communications on the same footing as traditional paper based communications and to give equivalent effect to electronic signatures as physical signatures.

These provisions have been implemented into English law by virtue of the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002. Rather than sweep away automatically all legislative provisions which require hard copy writing the Government elected to reserve power to itself to remove such requirements on a case by case basis using secondary legislation. Equally electronic signatures (as defined) will now be as effective as a physical signature although, as I say, for the most part the majority of commercial transactions under English law are unaffected by such developments.

Retention of Documents and E-mails

There is no general requirement to retain hard copies or electronic records. For most organisations retention policies are a matter of practicality and are developed with reference to the limitation periods set out by the Limitation Act 1980 which places a limit of 6 years within which most contractual or negligence claims must be commenced. However, this is somewhat arbitrary and caution must be exercised given that in some limited cases a longer limitation period will apply and also that the applicable limitation period may not always run from the date of the event giving rise to the claim but the date when the claimant should reasonably have realised the consequences of the event giving rise to the claim.

Subject to bearing these general principles in mind, and any industry specific requirements, companies are generally free to establish their own data retention policies. Companies must however be aware that once litigation in a particular dispute becomes a distinct possibility the rules change quite dramatically and companies must ensure that any material evidence is not destroyed. In this respect note should be taken of the recent Australian case involving McCabe against BAT (British American Tobacco). In that particular decision BAT were criticised for implementing a document destruction policy even though, at the time it was introduced, specific litigation was not ongoing. The judge remarked that the nature of BAT's commercial activities (the sale of tobacco) suggested that a partial reason for the document destruction policy might have been the destruction of adverse records and that, in the circumstances, BAT should not have implemented such a wholesale destruction policy.

Evidential Issues

It is perfectly clear that in the event of any dispute resulting in court proceedings all electronic documents and e-mail material relating to the dispute will have to be disclosed (as part of the process which used to be called discovery).

Historically, computerised records were not always admissible as evidence in court proceedings due to technical rules known as "hearsay". In reality judges simply viewed computer evidence with a significant degree of suspicion and did not know what reliance to place on the records. Only in relatively recent times has that position changed conclusively. Computerised records are now fully admissible in court proceedings as evidence by virtue of the Civil Evidence Act 1995 and the Criminal Evidence Act 1999. However, in determining the weight to be afforded to computerised records and e-mails the Judge is entitled to take into account all relevant circumstances. As a result it remains extremely important to be able to adequately demonstrate the security of the computer systems in question.

Information Offences

The Computer Misuse Act 1990 was introduced with the advent of the computer age and the realisation that computers were particularly susceptible to criminal attacks but could also be used as an instrument of criminal activity. Since its enactment the Computer Misuse Act has, however, been bedevilled by constraints inherent in its wording which have led to certain anomalies. I believe that a review of the legislation is currently being undertaken partly, I suspect, as a result of the UK's signatory of the Council of Europe Convention on Cyber Crime. This international treaty entered into between most of the major European countries and some others, notably the US, is a recognition of the fact that computerised crime is an international phenomena and, in the absence of harmonised provisions, criminals are likely to escape by operating through jurisdictions without the applicable legal framework. With this in mind, the Convention attempts to harmonise a basic set of computer related offences which include illegal access to computer systems, illegal interceptions of communications, interference with systems and data, computer related forgery and fraud, child pornography and copyright infringement. All of the individual offences must be committed intentionally and "without legal right".

The Convention also recognises the need for adequate processes and procedures to be in place to enable the authorities to react to criminal activity. With this in mind countries are required to put in place procedures guaranteeing expedited preservation of data and expedited mechanisms for the search and seizure of data.

One particularly important and potentially disturbing aspect of the Convention is that it expressly provides for corporate liability where there has been a failure by a company to supervise or control the use of IT facilities which in turn facilitates the commission by employees and other users of offences.

Although a signatory to the Convention it is apparently not

mandatory to implement the provisions of the treaty into English law although I suspect that this will be part of any review which takes place.

Monitoring E-Mails

It has traditionally been stated that no right of privacy exists under English law. Whilst historically that may have been the position the position now is quite different. First developments arose in the case of Halford against the United Kingdom involving the tapping of telephone conversations. In that particular case, the European Court of Justice ruled that Alison Halford, a senior police officer, had a reasonable expectation of privacy given the particular circumstances which prevailed at the time in the relationship between herself and her employer. Subsequent to that the UK enacted the Human Rights Act 1998 which became effective from 2 October 2000. That legislation effectively incorporates the European Convention on Human Rights into English law and specifically requires all public bodies, including the courts, to respect the fundamental human rights established by the Convention. One such right is respect for personal correspondence.

It became apparent that the rules governing the power of employers to monitor and intercept employee communications needed to be clarified. With that in mind, in accordance with powers created by the Regulation of Investigatory Powers Act 2000 the Government introduced the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 which became effective on 24 October 2000. This permits businesses to monitor or record communications without the consent of the individuals concerned to either establish the existence of facts relevant to the business, to prevent or detect crime or to investigate or detect unauthorised use. As a condition, the Regulations provide this can only be done where the business has made reasonable efforts to inform all direct users that this may be done. The guidance accompanying the Regulations suggests that in this context, "users" are only those who make direct use of the system, being employees and other users making direct use and not those third parties making inward communications. Many businesses reserve a contractual right to audit both computer and telephone use. However, it is now clear that such a blanket reservation of rights may not be effective.

The Information Commissioner regards the exercise of such powers as being potentially in conflict with the Data Protection Act. She argues that the right to respect for correspondence creates substantive limitations on employers which cannot be avoided through advanced warnings. The Information Commissioner has issued a draft Code of Practice offering guidance on monitoring employee communications. The draft has caused a great deal of anxiety amongst the business community due to the fact that businesses are concerned to protect the security of their information and information systems, preserve their goodwill both amongst customers and employees and avoid liabilities which could potentially arise from employee misuse of information systems.

According to a number of commentators the Code would prevent all forms of monitoring and virus detection software which are regarded as essential to protect essential business operations. For this reason, publication of the final form of the Code has been delayed considerably. The Information Commissioner is facing considerable pressure to make the Code slightly more balanced although, to date, she has steadfastly refused to bow to this pressure. Whilst the final version of the Code is expected by the end of June, all businesses would be wise to ensure that information gathering exercises have a legitimate purpose and invade privacy as little as possible. Businesses should first satisfy themselves that there is a real problem which needs to be addressed and undertake monitoring and interception only where there is a real business need. Any such monitoring and interception must be proportional to the threat posed.

Intellectual Property Developments

The European Community have recently published a draft Directive on patent protection for so called "computer implemented inventions". This is the first step in the conclusion of a long running debate and consultation process which arose out of the fact that, firstly, the law and practice relating to the patentability of computer software was uncertain and, secondly, there was some suggestion that the increased availability of patent protection for software in countries such as the United States was placing European technology companies at a competitive disadvantage. Under the existing legislation applicable in England, software is expressly stated to be outside the ambit of patent protection. However, evidence suggests that a very significant number of patents are granted where software constitutes a very significant component of the invention claimed.

The draft Directive proposes that a computer implemented invention which makes the necessary "technical contribution" to the current state of the art will be patentable. However, under the proposals computer programs themselves would not be patentable and neither would pure business methods. As with most European legislation these proposals will take some time before they are formally finalised and adopted thereafter there will still be a period for the necessary amendments to be reflected in domestic UK legislation.

The Copyright Directive

The Directive on the harmonisation of copyright and related rights in the information society has to be implemented into English law by 22 December 2002. Since English copyright legislation has only relatively recently been updated, the implementation of the Directive is not likely to have too much of an impact in this country. The Directive clarifies the extent of the existing rights of reproduction and distribution of copyright works and introduces a new right of "communication to the public". The Directive also requires that member states provide appropriate legislative protection for so called copy protection devices and other technical measures (such as digital watermarks) utilised by copyright owners as well as so called "rights management information". A draft statutory instrument is expected very soon.

Database Right

Historically the legal protection afforded to collections of information was uncertain and varied considerably between different European countries. Some, such as the UK, afforded databases copyright protection whereas others required quite high levels of originality and skill with the result that many databases which had received very significant levels of investment went without protection. To cure this problem the European Community adopted a Directive which created a new database right. The aim of the Directive was to provide a uniform level of protection. Quite recently we have seen the first case concerning the interpretation of the Directive involving the British Horseracing Board against William Hill. The case

involved the database compiled by the BHB of comprehensive information relating to horses and racing fixtures which bookmakers then utilise for the purposes of their betting businesses. At first instance in the High Court it was found that the bookmaker's publication of racing information extracted from the BHB database infringed the database right as it constituted "repeated and substantial extraction and re-utilisation of data" as prohibited by the Directive. Most commentators seemed to suggest that this was an entirely predictable outcome and was consistent with the purpose of the Directive. However, William Hill was not to be deterred and consequently appealed. Acknowledging that a number of Courts across the European Community had recently had cause to interpret the Directive and had come up with varying conclusions the Court of Appeal referred a number of questions regarding the interpretation of the Directive to the European Court of Justice. The result of this referral is still awaited.

Account Aggregation

Providers of financial services may be aware of the emergence of new personal finance account aggregation services. These are essentially services whereby service providers undertake to provide to individual customers, (usually over the Internet) a consolidated financial picture taking information from all of the accounts held by the individual in question. Such services give rise to a number of intellectual property and other legal issues. For example, by signing up for such a service the customer may be committing a breach of their financial providers' terms and conditions, the service provider may be committing a breach of the Computer Misuse Act by gaining unauthorised access to computer material, downloading and compiling financial information from financial services companies could amount to a breach of copyright/database right and, finally, such activities could constitute a breach of section 55 of the Data Protection Act involving the obtaining of personal data without the consent of the data controller (the financial services company).

On-Line Trading

The UK should have implemented the e-commerce Directive by 17 January 2002. However, we have not met that deadline and separate consultations on the implementation on the Directive in the Financial Services Sector and elsewhere only ended on 2 May.

The Directive sets out certain mandatory information which must be provided to customers where on-line trading is involved. In addition, the Directive seeks to resolve the conundrum as to which law should govern the activities of those that provide goods and services electronically. The Directive adopts the so called "country of origin" principle whereby the service provider has to comply with the laws of the country where it has its "fixed establishment". In practice this means where the service provider has the centre of its activities and where effective management control is exercised. Importantly, the location of the technology is not the key criteria. The adoption of this principal is aimed at making it easier to conduct international e-commerce. However, one aspect which has caused some concern is that the principle does not apply in relation to laws protecting the interests of consumers. Potentially, this means that those providing information services to consumers will still have to comply with the laws of each individual member state.

Tax

There have been two recent developments which might be of material interest to those involved in the provision of information relation services. In the budget of April 2002 the Chancellor publicised the introduction of a new regime providing company tax relief for the cost of the acquisition and development of intangible assets including intellectual property rights and goodwill. This regime will therefore be of direct relevance to those who provide information related services and who spend large sums on acquiring rights in respect of information.

The other development is the adoption of a Directive on the application of value added tax to electronically delivered services. This Directive has to be implemented in member states by 1 July 2003. It is aimed at ensuring a level playing field for both EU and non EU based businesses. For the first time providers of on-line services based outside the European Community will have to register for, charge and account for VAT. Previously, they had been at a considerable advantage by not having to charge VAT to customers.

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should either be on double spaced, single-sided A4 paper, e-mail, or in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality monochrome photograph, or electronic image.

Submission Deadlines

Spring Edition	7th February	Autumn Edition	7th August
Summer Edition	7th June	Winter Edition	7th November

The Benefits of CAATs

Lee Ann Kalaba

The use of computer assisted audit techniques (CAATs) is gaining popularity, not only with audit departments, but also with the clients they serve. However, some may argue that the cost – both in dollars and time spent implementing and training – of these techniques is not justified, especially during a time of layoffs and budget cuts. In actuality, CAATs provide added value to clients because they result in a complete picture of a system and/or an organization's transactions. As a result, one data analysis project should prove the benefits of CAATs to both the engagement team and its clients.

As an example, consider the review of revenue, specifically customer payments. During a typical financial statement review, the external auditors obtain the ending balance in the revenue account and a detailed listing of transactions. The ending balance is used in an analytical review, comparing current revenue to the same revenue in the prior year. If the variance is reasonable, based on criteria determined by the auditor, specific transactions are selected and confirmation letters are sent to substantively test the accuracy and existence of the transactions. If the variance is not acceptable, further investigation, usually by inquiry and observation of documentation, is conducted to determine if there are any unusual transactions making up the variance. Once the variance has been explained to an acceptable level, confirmation of sampled transactions is performed.

Auditors then base their conclusions about the reasonableness of the revenue balance on analytical review and customer confirmations. The following questions can be asked about the thoroughness of this analysis:

- Does this analysis provide a sufficient level of comfort?
- Have the auditors identified all the variables that might possibly affect revenue to ensure there is nothing unusual in any sub-categories?
- Have the auditors performed anything that the clients could not do for themselves?
- Have the auditors provided any benefit to the clients?

Most likely, the answer to these questions is "no." This is where CAATs come into the picture. With software such as ACL, CaseWare IDEA, and Microsoft Access, auditors can analyze 100 percent of the transactions for every category possible, based on the fields that exist in the database associated with the application that records revenue. This is a gigantic leap over analytical review of the ending revenue balance and customer confirmations, which only take into consideration a small percentage of the transactions.

Consider that when using automated software, the auditor can classify (summarize data based on categories of information), stratify (break out the number of transactions in specific dollar ranges), and provide statistics on all transactions. This basic analysis can be extremely useful to clients.

Audit Tool Functions

To illustrate, classifications of 100 percent of revenue data can provide the following information:

- Transactions per customer.
- Revenue per customer.
- Receivables per customer.
- Revenue per day/week/month/season.
- Insufficient funds per customer.
- Revenue per type of customer (ie, commercial, residential, etc).
- Revenue per type of service or product.
- Write-offs per customer.

Auditors can also classify based on more than one category. For example, they can classify revenue per customer per month, or revenue per product per customer. This type of analysis may provide the client with some insight into the behavior of its customers, as well as help to identify items that appear unusual based on more well-defined classifications of data. At the very least, auditors can present the data in a manner that their clients have probably never seen.

Besides classifications, auditors can stratify amounts on any interval. This helps identify the ranges in which customers spend their money. If auditors stratify revenue in $50 segments, they may see that most customers spend between $250 and $300. This may lead the client to ask what can be done to lure more low-dollar customers.

Auditors can perform similar analysis on quantity to determine if customers tend to buy a small or large amount of items or services, or on the number of transactions per customer to see if they are repeat buyers. Additionally, they can use automated audit tools to review for duplicates and missing transactions (for those that are numbered sequentially), testing for both over and understatement of revenue.

In terms of how this contributes to audit procedures, once auditors have analyzed 100 percent of the population, they can then determine items that look unusual. They may choose to document all transactions that look unusual or perform substantive testing by reviewing the subset of data.

Let's say that auditors decide transactions greater than two times the average transaction amount appear unusual. Well, they can separate these transactions and then sample and test the subset of the population. However, auditors should be careful when they extrapolate. The base of this extrapolation becomes the subset population, not the total revenue amount.

A similar approach can be taken for all of the analysis auditors perform. Essentially this removes items that appear valid and focuses testing on items that are more likely to contain errors.

Detecting fraud

What about crafty, fraudulent transactions that are meant to blend in with the data? Well, particularly in ACL, auditors can review for these types of transactions using Benford's analysis. Benford's Law basically states that there is a specific probability of the first digit of a number being 1, 2, 3, etc. Auditors might think that each digit is expected to be the first digit of a number one-ninth of the time. But this is not true. The number one actually appears as the first digit approximately 30.1 percent of the time, two is 17.61 percent, three is 12.49 percent, and so

on. Auditors can find more in-depth explanations and the formula itself at ITAudit, AuditNet, and various other Web sites, using search engines to find related documents.

Using this probability of occurrence for the first digit, auditors can analyze the occurrence of digits for their transactions. By isolating digits that occur more often than expected and substantively testing them, auditors may uncover fraud, errors, or unusual transactions. Note that Benford's analysis alone does not provide concrete evidence of wrongdoing. Auditors must test the transactions to determine if there is an irregularity.

Conclusion

As you can see, the application of CAATS is widespread, flexible, and comprehensive. By analyzing 100 percent of transactions, focusing testing on subsets of data that appear irregular, and presenting the information to clients in a new format, the answer to the previously asked questions about the thoroughness of the analysis should be "Absolutely."

Lee Ann Kalaba is the Lead IT Auditor at Tucson Electric Power Company. She has more than six years experience in business, public accounting, IT auditing, and automated audit tools. As a CPA and graduate of the Berger Entrepreneurship Program, Karl Eller Center (University of Arizona), Lee Ann has a well-rounded perspective on IT auditing.

The Web Page

Hoaxes, scams and the urge to ultracrepidate

Andrew Hawker
University of Birmingham

The mark of a good scam is that you fall for it. By the time this happens, of course, it is usually too late to retrieve your money, or your dignity, or whatever else you may have lost. Indeed, in the very best scams you may not even realise that something has gone missing.

The mark of keen professionals involved in Information Risk Management is a tendency to hold deep suspicions about life and the universe in general, and technology in particular. Not for us the cheerful handing over of credit card numbers or bank details, in response to a plausible email from Africa. The spurious virus warning, the latest urban legend, all these things bring only a wry smile to our lips. We spot these things a mile off. We are the great Guardians of Disbelief.

This kind of drift into complacency needs, perhaps, to be challenged from time to time. One way of doing this is to take a look at some of the many web sites which catalogue Internet ruses, hoaxes and scams. Many of the incidents which are cited are sketchy and anecdotal. However, they should not be underestimated as a source of ideas. For example, what kind of stories does it seem that people want to believe? Do the stories actually suggest ways in which fraud might be attempted in your business?

Take the case of the employee with the wheelbarrow.

> Every night for twenty years, an employee left the factory pushing a wheelbarrow full of waste materials. On the day of his retirement, the guard told him: "I've seen you walk out of here every night, and I know you've been stealing something. But I can't for the life of me see what it is!" "Wheelbarrows" said the employee.

This is a classic tale of misdirection, which prompts some interesting thoughts when you are looking at ways of regulating traffic through a firewall, or policies on Internet access. It tells you never to assume that something is innocent because it is familiar. It makes you think laterally about the risks which you may be facing. Other stories can have a more direct relevance, such as the one about the embarrassing Post-it.

> A tourist complained to an airline about finding cockroaches on one of their aircraft during a flight. He received a lengthy and apologetic letter, explaining how concerned the airline was about this problem, and the measures they were taking to eliminate it. Unfortunately, he also found, stuck inside the envelope, a post-it note which had been written by the PR manager to his secretary. This read: "Just send this jerk the standard cockroach letter".

This too has some electronic parallels. For example, the Word document that you are sending your client as an attachment may contain all kinds of buried information about previous drafts, or even perhaps some scurrilous annotations by your colleagues. Constant hitting of the email "reply" button is also a good way of forwarding a whole sequence of messages which have stacked up between various senders, perhaps going back a lot farther than you intended.

Needless to say, the above stories have been taken from hoax and scam web sites. Here is another one, aimed more simply at scaring readers.

When you go to an automatic teller machine to make deposits, make sure you don't lick the deposit envelope. A customer died after licking an envelope at Yonge & Eglinton. According to the police, Dr Elliott at the Women's College hospital found traces of cyanide in the lady's mouth, and the police traced the fatal poison to the glue on the envelope. They then did an inspection of other envelopes from other teller machines in the area and found six more.

Such "urban myths" can gather momentum quickly, because of the speed with which they are passed on via the Internet. The best stories are intriguing, scary, and full of circumstantial detail. Some, like the tourist who was drugged and relieved of a kidney, or the cinema-goer stabbed with an AIDS-infected needle, have re-surfaced countless times, with various different alleged victims and settings. The appeal to morbid curiosity is much the same as that exploited in the heading of a hoax virus email, where the aim is to make people feel guilty if they do not take immediate action to warn their friends or colleagues.

A useful introduction to urban myths, with examples of some of those that have stood the test of time, can be found at **urbanlegends.about.com** A more systematic directory of stories currently doing the rounds can be found at a site run by the Computer Incident Advisory Capability of the US Department of Energy, at **HoaxBusters.ciac.org**. The CIAC site provides pointers for some, but not all, of its stories, for those who want to find more about the supporting evidence (or lack of it). Ultimately, of course, it is unlikely that any story can ever be completely disproved. The "Urban Legends Reference Pages" at **www.snopes2.com** wrestle with this problem. Each story is given a colour-coded rating. This may be simply "True" or "False". Many of the ratings, however, are in between, denoting "undetermined or ambiguous veracity", or "indeterminate origin".

For hoax viruses, a good source of reference is again the CIAC site (above). Details of around 140 hoax viruses can be found at **www.symantec.com**, while nearly twice as many are indexed at **www.europe.f-secure.com**.

Being able to identify a hoax or legend does not of course enable you to stop it in its tracks. By the time you have discovered its arrival, it may have been forwarded to half the staff in the company. However, it can be useful to be able to show just how old and tired a particular story is, with a view to embarrassing everyone who enthusiastically passed it around.

Hoaxes waste time and create anxiety, but e-commerce scams are intended to cause more direct damage. For example, one recent survey of Internet vendors found that fraudulent transactions accounted, on average, for a loss of about 3% of revenues: (see **www.cybersource.com**). Both vendors and buyers need to be aware of the kind of tricks which can be played, and a good first port of call for reference material is the site run by the US Federal Trade Commission at **www.ftc.gov**. The FTC has now brought a number of successful prosecutions for Internet fraud, and also tracks the steady stream of complaints that it receives from consumers. Coverage of e-commerce issues is to be found mainly in its pages on Consumer Protection. The FTC provides a list of "Top 10 Dot Cons", concluding each one with a simple piece of advice for consumers. It also nominates a "Dirty Dozen" of the scams most likely to arrive via bulk email. There is a search facility, that can be used to find details of the FTC's position papers and submissions on matters such as cramming, identity theft and cross-border Internet fraud.

The Scambusters site at **www.scambusters.org** offers another view of the current "Top 10 Scams", and provides a free monthly newsletter, that is also archived on the site. This site is well presented and has a search facility, but the material is of variable quality, and much of it is very specific to cases and legislation in the USA.

A site operated by the US National Consumers League at **www.fraud.org** has useful information on the problems which can arise with on-line auctions. However, it is generally a bit haphazard in its coverage. The UK Consumers' Association has a limited amount of advice for on-line shoppers, at **www.which.net**, which tries to steer a rather less alarmist course than some of the other sites.

Finally, for those who would prefer to download a report on techniques available to combat Internet fraud, a Fraud Prevention Guide can be obtained in Adobe format from **www.clearcommerce.com**, on registering with your name and address.

This just leaves the question of ultracrepidation. Learned readers of this journal will know that this means giving advice which goes beyond the scope of your expertise. Web sites frequently seem to ultracrepidate. At least, this may or may not be the right word to describe what they do. For example, a common thread in advice on web fraud is that statements should never be taken at face value, but should always be carefully checked out. Yet the same site may offer absolutely no evidence or authentication for the claims it is making.

Such are the paradoxes of the Internet. Is it possible that an anti-hoax web site might actually be hoaxing you? Or could it be well out of its depth in terms of the technical information it provides? If so, would it be ultracrepidating? Or would another word be more appropriate?

If you can help to resolve this question, please do send your comments to the Journal Editor. (But beware. You have no reliable information as to who, or where he is. Could it be that he is just another Internet hoax?).

BCS MATTERS!

Colin Thompson
BCS Deputy Chief Executive

Colin Thompson, BCS Deputy Chief Executive, reviews some of the current BCS news items. Further information on these or any other BCS related issues may be found on the BCS Web site (http://www.bcs.org)

Information is also available from Customer Services at The British Computer Society, 1 Sanford Street, Swindon, SN11HJ (e-mail to marketing@hq.bcs.org.uk)

New Chief Executive takes over

May saw the handover of the BCS Chief Executive responsibility from Judith Scott to David Clarke. Judith has occupied the top job since 1995 and has seen the BCS through a period of dramatic transformation. Her achievement is perhaps best reflected in the income statements for the Society over the last 7 years. In 1995 our total income was just over £4 millions of which approximately half was from membership subscriptions. The accounts for the financial year just closed are likely to show an income figure in the region of £12 millions, of which membership subs account for only 20%. David Clarke will not be short of challenges over the next few years but he takes over a Society with a very sound financial position and an excellent set of products and services.

BCS Connect Rolls out

In the last edition of this newsletter I mentioned that user acceptance testing was in progress for a major enhancement to the BCS Web capability. That testing is now complete and the new web service is being rolled out, under the label BCS Connect.

The aim is to put Web-based services at the heart of the relationship between the society and the IT community and the new service represents the biggest investment in service to members and to the wider IT community in the Society's history.

The BCS was one of the first professional bodies to set up a website. Since that launch in the mid-1990s the site has grown to more than 5,000 pages and almost 40,000 unique visitors a month. The new system is designed to add value by providing a much more interactive and intelligent service, with the Web front end linked to The BCS' back-office systems. An essential part of this will be the linkage to the main database of all BCS members and other contacts, to ensure that services are more closely tailored to the interests and access rights of individuals.

The heart of the new system is an information management system, providing users with the latest information that may be of interest to them, based on the society's knowledge of their requirements and driven from the core administrative systems. Built-in security will ensure that a single log-on will enable registered users to reach all the areas of the site and view all the documents for which they have access permission.

BCS Connect is a very ambitious programme that will change almost every aspect of BCS business. The full range of facilities is being developed and delivered in a series of phases, extending over several years.

Stage one facilities, now being rolled out, will include a list server, online updating of individual records, similar facilities for updating member records by branches and specialist groups, online registration for the new BCS forums, threaded discussion groups, and standard reports for branches and specialist groups.

Around 40% of BCS members notify a change to some aspect of their personal record each year, and online updating should improve both member service and administrative efficiency.

Online forum registration will allow both BCS members and others to join one or more of the three new forums, introduced last October to serve three main sections of The BCS' community: Education and Training, Engineering and Technology, and Management.

Web-based discussion groups will provide one of the main channels through which BCS members can engage with each other and with the society itself in the future.

Online updating for branches and specialist groups will enable each one to update the address details of its own members. This facility will open the prospect of having a single central database holding the contact details for everyone associated with The BCS.

Online reports will ensure that branches and specialist groups are able not only to access essential information relating to their memberships but also to have that information updated dynamically on demand from the latest data recorded on the central database.

Effective security is an essential feature of BCS Connect: we shall therefore be asking all users to register before they can access any of the new facilities. After completing an online form, each applicant for registration will receive a letter providing a unique personal identification number and instructions on completing the application process. Keying the number will allow the creation of a personal password which, with the membership number, will provide the main access control.

The initial registration process represents a very considerable task for BCS staff, and we plan to spread the work over time to ensure that it can be handled and supported effectively. Over the next two to three months e-mail messages will be sent to groups of members, inviting them to complete the registration. Once the bulk of each group has been dealt with, invitations will be issued to the next group, and so on until all members with known e-mail addresses have been covered.

Facilities to be introduced over the next few months are an essential foundation for the BCS Connect service, and major developments will be built on that foundation. Candidates for early development include membership renewals, registration for professional examinations and BCS Information Systems Examinations Board qualifications, continuing professional development and personal experience record facilities, reservations for conferences and seminars, Internet trading, and committee and specialist group management facilities.

ECDL marches on

The European Computer Driving Licence, the international computer skills qualification launched in the UK by BCS

four years ago, goes from strength to strength. The qualification, which already has nearly 2 million candidates in 60 countries, is set to be enhanced further after a recommendation by a key European Union committee, the High Level Group for Employment and Social Dimension of the Information Society, that the European Commission accept it as the standard diploma for basic computing skills.

UK organisations including the National Health Service, the Ministry of Defence, the Bank of England and major companies are adopting the qualification as standard. People can take it via 2,000 UK training and testing centres. And if a recent BCS survey is to be believed, UK candidates rate the qualification very highly. Around 10,000 ECDL holders, from both the Further Education and the Corporate sectors, were surveyed to gauge satisfaction with the programme leading to ECDL qualification.

Apart from a gratifying 95 per cent satisfaction rating, almost two thirds of those polled chose ECDL because of its broad recognition as a computer skills qualification. In addition, 97% said they would recommend ECDL to family, friends and colleagues and 87% were interested in an ECDL Advanced qualification. The recent launch of that advanced level qualification is further evidence of the strength of the ECDL brand. Following a six-month roll-out period, a national infrastructure of 120 test centres able to provide the new qualification is now in place.

ECDL Advanced is designed for candidates who want further recognition of their skills, in order to progress their careers, to make the most of their computers or just to validate their knowledge. Take up of the new qualification has already exceeded expectations and the launch event at The Hilton Hotel, Kensington, London, on 17th April 2002 saw the BCS presenting the one thousandth certificate for an ECDL Advanced exam undertaken.

BCS member survey

BCS members strongly value the professional status and the information services that membership provides and would like the Society to step up its campaigning on IT issues. These were two of the main conclusions to emerge from another survey conducted by the Society. 3,000 replies were received to the first of a planned series of annual member surveys.

Members saw the principal role of The BCS as setting and promoting professional standards (74%). Representing the profession to government and industry (52%) and supporting and encouraging the advancement of information systems knowledge (42%) were also felt to be important.

Asked what they thought The BCS' role should be in the future, 73% of members felt the setting of professional standards should continue to be key, but many would like to see more campaigning: representing the profession to government and industry (69%) and initiating and encouraging debate on IS issues (47%).

Most BCS members pay for their own membership (77%). Most are satisfied with the current BCS member benefit package (67% are very or quite satisfied), especially the free copies of trade journal Computing and the membership magazine, The Computer Bulletin, plus personal networking opportunities and the Continuing Professional Development scheme.

The survey highlighted how members get involved with The BCS in many ways. Over half have used the web site in the last 12 months, 22% have attended a branch meeting and 12% a specialist group meeting. There is also interest in the new BCS forums.

More than 70% of members currently work in IS, mainly in management, systems development or technical advice and consultancy; a further 11% are in education or training.

Chinese agreement

Extending the international influence of the BCS is set to be one of the key themes of John Ivinson's Presidency and John has played a major role in the negotiation of a Memorandum of Understanding between the Society and the China International Exchange Foundation, an agency of the Chinese Government.

The document was signed by John at a ceremony at the Society's London office attended by a delegation led by the Chinese ambassador to the UK, Ma Zhengang, and the vice-general director of the State Administration of Foreign Experts Affairs, Zheng Huaisheng.

It is hoped that the non-contractual document will provide a framework for future cooperation, possibly including agreements for the use of BCS professional development products in China.

BCS small business resource

As part of the objective of increasing the on-line services, the BCS has launched a free online news and information resource aimed at the UK's small business sector. The new dedicated BCS microsite homepage will provide small and growing businesses with access to significant business national and European daily news stories as they break together with features and advice.

Developed by small business brand Business Europe, the microsite is also designed to provide assistance to help small businesses in cutting through red tape, identifying new business leads, taking advantage of e-commerce to run their businesses more effectively.

The advice on the site focuses around five key areas: technology; e-commerce; sales and marketing; finance; human resources. Each of these resource areas contains a glossary of terminology and easy to understand 'how to' guides. There are also case studies of companies so that owner-managers can gain an insight into real life success stories.

Twice a day the microsite will be updated with news of legislation, events and developments all reported from the point of view of the UK's small and medium sized businesses. In depth features examine topical business issues.

And finally……

More changes at the top – this time the annual changes of the senior Officers of the Society. Geoff McMullen completes his presidential year in October and Council has now confirmed that he will be succeeded by the Deputy president John Ivinson. Council also approved the election of Professor Wendy Hall to follow John into the Deputy Presidents seat. Wendy, currently Vice President for knowledge services, is Professor of Computer Science at the University of

Southampton. She was founding Head of the Intelligence, Agents, Multimedia (IAM) Research Group in the University's Department of Electronics and Computer Science and is currently Deputy Head of Department.

Wendy is a director of Active Navigation Ltd the company through which the award winning open hypermedia system, Microcosm, was marketed, and through which her group's work on Web link services has also been exploited as part of the new Portal Maximiser product. As well as hypermedia and web technologies, her research interests include multimedia information systems, digital libraries, user interfaces and agent-based systems. She has published over 200 papers in these areas.

Wendy was awarded a CBE in the Queens Birthday Honours list in June 2000 and was made a Fellow of the Royal Academy of Engineering in the same year. She is a Fellow of both the BCS and the IEE, and is also an active member of the ACM. She is currently the holder of a prestigious 5 year EPSRC Senior Fellowship, and was a member of EPSRC Council from 1997 - 2002.

Minutes of the Annual General Meeting of the Information Risk Management and Audit Specialist Group held on Tuesday 14th May 2002

1. Approval of the minutes of the AGM held on the 15th May 2001.

The minutes of the AGM held on the 15th May 2001 were approved. Proposer: Siobhan Tracey; Seconder: Peter Biss.

2. Chairman's report.

John Bevan – thanked Siobhan Tracey for deputising while John was dealing with his family problems. This episode in John's life is over now and things are beginning to return to normal. This year John is able to give the group his full attention.

Last year's meetings

The meetings held in 2001/2002 were:

Date	*Title*	*Attendance*
October 2nd	"Windows 2000 Security"	32 (evening)
November 12th	"Outsourcing & Out of Control Projects"	55
December 4th	"Network Security & Management"	36 (evening)
January 29th	"Internet Security"	69
February 12th	"The Subversive Spreadsheet"	40 (evening)
March 5th	"The System's Down-Again!" (clashed with another conference)	32
May 14th	"Data & The Law"	40 (evening)

There has been a consistently good turnout for the evening meetings, most reaching capacity for the room size.

Thanks to KPMG for the excellent room and the facilities. We have been offered the use of the room next year.

Membership

Membership has grown again this year from 245 members in May 2001 to 307 as at May 2002. This was helped by the promotion of the group to local government, which produced 14 new members.

This year the group will be chasing up lapsed memberships and sending out the usual reminders to renew memberships in July.

The web site is now up and running which will help to promote the group.

Administration

Janet Cardell-Williams was thanked for her hard work as Administrator and in helping with the name change, which went smoothly.

IRMA Journal

John Mitchell was thanked once again for consistently and efficiently turning out the Journal on time.

Thanks to the Committee members

Thanks to Raghu Iyer who is retiring as Secretary but will be staying on the Committee.

Mike Demetriou who is also retiring as Treasurer, was thanked for his work.

Thanks to Alan Boardman for setting up the Web Site.

Thanks to the Committee members who helped organise the meetings

3. Treasurers Report

Given by Mike Demetriou. Proposer: Monica Edmonds: Seconder Peter Biss.

This year there has been an overall loss of £6,400. This was due to the rising costs of meeting venues, the name change and the big promotion drive to Local Government. The admin costs have gone up, as has the cost of producing the Journal due to the growing membership. Also, interest rates have gone down on the deposit account so we are earning less on the money deposited. A change to a higher interest account is a possibility.

However even after reporting a loss this year the bank balance is still a healthy £30,000.

Thanks was given to Janet for handling membership subscriptions.

4. Election of the Officers

Chairman: John Bevan
Deputy Chairman: Peter Biss
Proposer: Siobhan Tracey: Seconder Celeste Rush

Raghu Iyer is standing down as Secretary
New Secretary: Siobhan Tracey
Proposer: Monica Edmonds: Seconder Mike Demetriou.

Mike Demetriou is standing down as Treasurer
New Treasurer: Jan Lubbe
Proposer: John Mitchell; Seconder: Siobhan Tracey.

5. Election of Honorary Auditor

Chris Wright was Honorary Auditor last year. In his absence it was hoped he will once again act as Honorary Auditor for another year.

6. Appointment of Committee

Thanks to Mike Demetriou and Paul Plane for their hard work as both are leaving the Committee.

7. Plans for next year

Dates for meetings to be added and finalized. Priorities are to run a good programme of meetings, to continue publishing the Journal, which by the way is looking for a new Editor (Volunteers welcome). To continue chasing up memberships and promoting the group meetings.

8. Any other Business

The BCS has reorganized itself and has a new Security Panel. Willie List, its Chairman, is aiming to make the Panel more approachable, with more involvement from IRMA and the ISSG. John Mitchell will represent IRMA on the Security Panel.

BS15000 – John Bevan and John Mitchell to be in contact.

There being no other business the meeting closed at 16.40.

Chairman's Report – John Bevan

I was not able to be an active chairman in the past year because of a serious illness within my family. I could not give the group the attention it needs. Siobhan Tracey was drafted in as Deputy Chairman to assist. I should like to thank her both for her assistance and for preparing this report on the year concerned.

As we look back on the previous year I should like to highlight the following:

Membership

We have experienced a useful increase in membership of 62 relative to this time last year.

Paid up members at 14.05.02 – 307
Paid up members at 14.05.01 – 245

The increase in membership was partly due to the CIPFA promotion resulting in 14 new members and 3 new delegates and a drive by our administrator to get lapsed members to rejoin. We recorded more persons attending our briefings as joining the group.

I would like to remind our members that the renewal notices will be sent out in July.

If you know anyone who would be interested in the group's activities, and would like to join, please direct them to our web site at www.bcs-irma.org.

Meetings

We held 7 meetings last year – 3 full day and 4 evening (marked (E) below)

Title	*Date*	*Attendance*
Windows 2000 Security (E)	2nd October 2001	32
Outsourcing & Out of Control Projects	12th November 2001	55
Network Security & Management (E)	4th December 2001	36
Internet Security	29th January 2002	69
The Subversive Spreadsheet (E)	12th February 2002	40
The System's Down – Again!	5th March 2002	32

We will again be having a joint meeting with the Institute of Chartered Accounts in England & Wales IT Faculty next year. There is a room-size limit on the numbers attending the evening sessions and most such meetings have reached this limit.

We would like to thank KPMG for providing the venue for the evening meetings. The room size and the facilities are excellent and we are very happy that they have offered the use of these rooms for next years meetings.

We introduced a buffet after the evening meetings, in order to allow members to meet each other, the speaker, and the management committee. This was considered to be a successful innovation.

Name Change

As you are aware the Group changed its name from CASG (Computer Audit Specialist Group) to IRMA (Information Risk Management & Audit) during the current year. The new name has been well received both by our members and by the BCS. The name changeover went very well mainly due to the great work performed by our administrator Janet Cardell-Williams.

Thanks

I would like to propose a vote of thanks to all those who sat on the Committee and helped to organise the 2001-2002 programme of events. A draft programme of meetings for 2002-2003 has also been prepared and circulated.

I would also like to propose a vote of thanks to Raghu Iyer, our retiring secretary, who has served this group and our members very well over his years of stewardship. Raghu has kindly agreed to stay on the committee for this year.

Our thanks also go to Mike Demetriou, our retiring treasurer.

Other Items

We finally got our web site fully functioning. (www.bcs-irma.org). The facility is now available to book all our events. If you visit the site you can also find a very good reference section under "Resources". The web site has averaged over 3000 hits per month with a high of almost 5000 in January. The web site has been well received by those who have visited it. Our thanks go to Allan Boardman.

In the late April mailing to members I appealed for help in assisting the BCS Security Panel to review proposed changes to legislation, standards, and guidelines that affect IRMA members. As at May 14th I am pleased to report that I have received 11 responses, with more probably to come. I shall from time to time report to members on progress in this new pro-active SG role.

Report from the Cash Box

Mike Demetriou

Commentary

The group made a loss of £6,426 (pre-tax) from its activities during the last financial year. However, our cash balances are still healthy at £30,333 and the Committee is actively looking at ways of productively utilising these to continue to offer high quality technical briefings, evening meetings and the IRMA journal that are of value to our members.

This reasons for the loss was a combination of factors. The increasing cost of venues and catering arrangements has eroded income from our full day events. We have endeavoured to keep the cost of these events to delegates down and there has been no increase for over 5 years. We are looking at alternative arrangements before reviewing our charging structure. We have also improved our evening meetings by providing refreshments after these to allow time for members to network and exchange ideas.

During the financial year we incurred costs for our re-branding exercise which included a new and much improved web-site. Additionally we undertook a marketing campaign aimed at the Local Government sector to increase our membership and attendance at events. As a result of these, and other constraints on Committee Members, more work has been required of our very able Administrator Janet Cardell-Williams.

On the positive side our membership income is up for the second year running and we intend to continue increasing the size of the group. Revenue from advertising has reduced but has been replaced by the companies offering our members discount for the training, events and seminars being advertised and so is seen as a direct benefit to them.

Producing this report is my final task as IRMA Treasurer as I am retiring from the Committee. I hand over the reins to my successor Jan Lubbe and I wish him and IRMA well for the future.

Income and Expenditure Account for the Year Ended 30 April 2002 (Un-audited)

	2001/02	2000/01
Income	£	£
Technical Briefing Sessions & other meetings	11,506	10,129
Subscriptions	5,030	4,470
Interest on Bank Accounts	881	1,266
Journal Advertising	470	1,483
Other Income		
Prior Year Items		
	17,887	17,348
Expenditure		
Technical Briefing Sessions & other meetings	9,125	12,651
Journal	7,525	6,263
Printing, Postage & other Administration Expenses	7,663	2,156
Prior Year Items		
	24,313	21,070
Profit/Loss for the Year	(6,426)	(3,722)

Fund Balance	£
Fund Balance at 1st May 2001	36,759
Add 2001/2002 profit/loss	(6,426)
Fund Balance at 30 April 2002	30,333

Since these accounts were prepared invoices have been received for catering at evening meetings held before the end of the finacial year, which are not included in the above accounts. This was because at the end of the 2001/2 accounting period it was not known either whether this expenditure would be invoiced, or how much might be invoiced. The relevant expenditure totals £873 and will be included in the 2002/3 accounts.

John Bevan – Chairman

Event Reports

Answers we need to questions we'd rather not ask

Journal Events Reporter, Rupert Kendrick, reports on the March seminar 'The System's Down Again!' which focussed on business continuity and disaster recovery.

Systems or network failure are events that are preferable to ignore than to address. In many organisations, the steps needed to address business continuity and disaster recovery are only taken in the middle of, or after, the crisis itself – when it is far too late. This seminar addressed key technological and operational steps that need to be considered when disaster strikes.

The organisers had assembled a formidable array of experts to tackle the subject. The event opened with a presentation from Andy Shan, senior manager, business continuity and availability, KPMG, who looked generally at business continuity. As we move from the industrial age to the knowledge economy, he said, preserving business continuity means protecting knowledge. In a recent survey, he quoted 25% of organisations had a 'down time' tolerance of only 2 hours and 60% said their recovery objectives had not been met. Priority therefore needs to be given to systems critical to an organisation's operation. A model needs to be established where risk is assessed and organisations can adequately react to disaster, control it and finally transform it into recovery. The message from KPMG is ' IT is an area you can solve in advance – make it one less problem so you can concentrate on people process and customers' He ended with a useful checklist:

- Is the business continuity strategy driven by events or clear risk assessment?
- Is enough understood about the infrastructure to know which elements are critical?
- What is the tolerance of customers and stakeholders for downtime?
- Does the risk management strategy address people processes and technology?
- Is their independent assurance business continuity capability is adequate?

Otto Winterskov, director, business continuity programmes, EMC (www.emc.com) addressed some technical issues. The value and importance of new solutions, he said, is that they can improve security and reduce costs. CIOs face a real challenge from customers who demand 24 x 7 service, global competition, and a continuous and integrated supply chain. Organisations need to ask themselves whether they have systems capable of meeting these challenges. In particular, they need to understand that disaster recovery is reactive and business continuity is proactive.

He suggested some practical considerations:

- e-mail is critical as without communications, the business cannot survive;
- ensure a facility for replacement of the primary site;
- back up all relevant information;
- test the procedure frequently.

He offered a checklist for business continuity on a local and remote basis. Locally, the organisation needs to ensure:

- platform integrity;
- business integrity; and
- recovery integrity.

Remotely, the organisation needs to ensure:

- data integrity;
- processing integrity; and
- encryption integrity

He ended with a demonstration of some of the most recent solutions developed by EMC, including EMC's Timefinder for back-up solutions; EMC's Symmetrix Remote Data Facility (SRDF) data mirroring for recovery solutions; EMC's SRDF Multi-HopCapability for enterprise integrity; and EMC's AutoIS Strategy for data storage management.

John Peel, sales consultant, Global Recovery Services, gave a valuable presentation approaching business continuity issues from a project management perspective. He suggested a five-phase methodology to implementation:

- project management;
- identification of business need;
- continuity or recovery strategy evaluation;
- development of a plan;
- rehearsal and implementation.

Testing and rehearsal is particularly important. Technical rehearsal will involve a test run of the support technology, but there must also be office recovery rehearsals – and that means the staff. Examples of technical testing might include: data restoration from back-up media; activation of back-up data and voice communications; verification of restored data and recovery of IT capability at an alternative centre.

Office rehearsal involves: an audit of the plan; plan 'walkthroughs', where staff absorb the plan procedures; scenario rehearsals; and simulation exercises. His experience was that office recovery rehearsals were more difficult to organise because of the reluctance of management to become involved, although this was now improving. If done well, he maintained, confidence and interest was generated at all levels.

Julian Heal, of Booker Cash & Carry Ltd, provided some 'real-life' experiences of his own organisation in suffering at the hands of business continuity incidents, in an amusing and self-effacing presentation. The principal threat arose from the weather or, as he put it, 'Rain, rain and more rain!' which on two occasions threatened a substation. On a third occasion, 'fire' was the problem – or at least, a fire alarm, followed by evacuation of the building and a potential system failure.

Not surprisingly, these experiences had been a sharp learning curve and some important principles emerged:

- test, test and test again;
- ensure that the organisation's hardware is adequate;
- ensure the operations team can recover;
- ensure that enough business staff are aware of the duties;
- ensure an awareness of disaster recovery issues and procedures throughout the organisation;
- involve audit and security.

The event ended with a helpful reminder of some of the practical implications from ***Siobhan Tracey, audit manager (IT), Iceland Plc,*** who approached disaster recovery and business continuity from the view of the auditor. She made the cogent point that a disaster recovery plan must be comprehensive, covering all aspects – not simply IT issues. These plans are the responsibility of the whole organisation.

She suggested some helpful guidelines; establish mission-critical IT systems; ensure adequate and appropriate back-up; check any third party agreements for validity and suitability; ensure user involvement at all levels; and ensure adequate communication at all levels.

She then produced a series of matrixes to record project management issues for hardware, software, employer/employee issues, and third party issues. She stressed the need for use involvement and adequate communication in particular. Moving on to the role of the auditor, she emphasised that the auditor's role is not to prepare the plan, but to assist and advise, and ensure that the plan is prepared, documented and communicated within the business.

Testing the plan is essential because, unless they are tested, complacency sets in. After testing, the results must be reviewed and procedures established to address any flaws. The auditor will be involved in all testing and should review the test plans to ensure they are comprehensive also ensuring they are valid and up to date.

When disaster strikes, the role of the auditor is to keep away, offering help only if it is sought. After the event, the auditor investigates the causes of the incident to see if any preventative measures could have been adopted and to conduct a post-disaster review to see what was done correctly or incorrectly and to ensure plans are amended appropriately. Unfortunately, she concluded, auditors cannot force users to adopt and implement plans – if they could, one suspects business continuity and disaster recovery would be much more effective.

HUMOUR PAGES

There's nothing more annoying than a report with spelling errors, but when I was a cub auditor I often found that my boss could be diverted from changing the theme of a particularly hard hitting report by the assiduous insertion of many spelling errors. He then spent all his time correcting the spelling errors and feeling that he had made a valuable contribution to the report whilst leaving my points intact! I was reminded of my young duplicity when I can across the poem below. Ed.

Eye have a spelling chequer
It came with my pea sea
It plainly marques four my revue
Miss steaks eye kin knot sea.

Eye strike a key and type a word
And weight four it two say
Weather eye am wrong oar write
It shows me strait a weigh.
As soon as a mist ache is maid
It nose bee fore two long
And eye can put the error rite
Its rare lea ever wrong.

Eye have run this poem threw it
I am shore your pleased two no
Its letter perfect awl the weigh
My chequer tolled me sew.

• •

Those of us who are forced to travel on the tube have long believed that London Underground staff's sense of humour is to announce that the service has been suspended due to an air traffic controllers' strike. Not so is seems as below are some genuine announcements made by tube drivers on the underground. Ed.

To the gentleman wearing the long grey coat trying to get on the second carriage, what part of 'stand clear of the doors' don't you understand?"

• •

At Camden town station (on a crowded Saturday afternoon): "Please let the passengers off the train first. Please let the passengers off the train first. Please let the passengers off the train first. Let the passengers off the train FIRST! Oh go on then, stuff yourselves in like sardines, see if I care, I'm going home."

• •

"Ladies & Gentlemen, upon departing the train may I remind you to take your rubbish with you. Despite the fact that you are in something that is metal, fairly round, filthy and smells, this is a tube train for public transport and not a bin on wheels"

• •

Driver: "I apologise for the delay leaving the station ladies and gentlemen, this is due to a passenger masturbating on the train at Edgware Road. Someone has activated the alarm and he is being removed from the train.

• •

"Ladies and Gentlemen do you want the good news first or the bad news?"
"The good news is that last Friday was my birthday and I hit the town and had a great time. I felt sadly let down by the fact that none of you sent me a card! I drive you to work and home each day and not even a card."
"The bad news is that there is a points failure somewhere between Stratford and East Ham, which means that we probably won't reach our destination. We may have to stop and return. I won't reverse back up the line – simply get out walk up the platform and go back to where we started.
In the meantime if you get bored you can simply talk to the man in front or beside you or opposite you."
"Let me start you off:
"Hi, my name's Gary how do you do?"

• •

"Please mind the closing doors....
"The doors close....The doors reopen.
"Passengers are reminded that the big red slidey things on the side of the train are called the doors.
Let's try it again, shall we?
"Please stand clear of the doors."
The doors close...
"Thank you."

• •

"I am sorry about the delay, apparently some nutter has just wandered into the tunnel at Euston. We don't know when we'll be moving again, but these people tend to come out pretty quickly...usually in bits."

• •

Here are some ideas to help you look busy – Ed.

1. Never walk without a document in your hands. People with documents in their hands look like hardworking employees heading for important meetings. People with nothing in their hands look like they're heading for the cafeteria. People with a newspaper in their hand look like they're heading for the toilet. Above all, make sure you carry loads of stuff home with you at night, thus generating the false impression that you work longer hours than you do.

2. Use computers to look busy. Any time you use a computer, it looks like "work" to the casual observer. You can send and receive personal e-mail, chat and generally have a blast without doing anything remotely related to work. These aren't exactly the societal benefits that the proponents of the computer revolution would like to talk about but they're not bad either. When you get caught by your boss - and you will get caught - your best defence is to claim you're teaching yourself to use new software, thus saving on the training budget.

3. Have a messy desk.
Top management can get away with a clean desk. For the rest of us, it looks like we're not working hard enough. Build huge piles of documents around your workspace. To the observer, last year's work looks the same as today's work; it's volume that counts. Pile them high and wide. If you know somebody is coming to your desk, bury the document you'll need halfway down in an existing stack and rummage for it when he/she arrives.

4. Never answer your phone if you have voice mail. People don't call you just because they want to give you something for nothing – they call because they want YOU to do work for THEM. That's no way to live. Screen all your calls through voice mail. If somebody leaves a voice mail message for you and it sounds like impending work, respond during lunch hour when you know they're not there - it looks like you're hardworking and conscientious even though you're being a devious weasel.

5. Look impatient and annoyed. One should also always try to look impatient and annoyed to give your boss the impression that you are always busy.

6. Leave the office late. Always leave the office late, especially when the boss is still around. You could read magazines and novels that you always wanted to read but have no time for until late before leaving. Make sure you walk past the boss' room on your way out. Send important e-mail at unearthly hours (e.g. 9:35pm, 7:05am, etc.) and during public holidays.

7. Sigh loudly for effect. Do this when there are many people around, giving the impression that you are under extreme pressure.

HUMOUR PAGES

8. Develop a stacking strategy. It is not enough to pile lots of documents on the table. Put lots of books on the floor etc. (thick computer manuals are the best).

9. Build your vocabulary. Read up on some computer magazines and pick out all the jargon and new products. Use the phrases freely when in conversation with boss. Remember: They don't have to understand what you say, but you sure sound impressive.

10. MOST IMPORTANT: DON'T forward this to your boss by mistake!

••••••••••••••••••••••••••••••

Stating the obvious – Ed.

In the edition of BBC's "Radio Times" for films broadcast during the period 27th April – 3rd May was the following entry: Saturday 27th April. Battle of Britain A worthy tribute to "the few" with spectacular air battles, a memorable re-creation of the blitz and a terrific cast ..... Contains violence.

••••••••••••••••••••••••••••••

Memorable Interviews

Vice Presidents and personnel directors of the one hundred largest American corporations were asked to describe their most unusual experience interviewing prospective employees:

A job applicant challenged the interviewer to an arm wrestle.

Interviewee wore a Walkman, explaining that she could listen to the interviewer and the music at the same time.

Candidate announced she hadn't had lunch and proceeded to eat a hamburger and french fries in the interviewers office.

Candidate explained that her long-term goal was to replace the interviewer.

Candidate said he never finished high school because he was kidnapped and kept in a closet in Mexico.

Balding candidate excused himself and returned to the office a few minutes later wearing a headpiece.

Applicant said if he was hired he would demonstrate his loyalty by having the corporate logo tattooed on his forearm.

Applicant interrupted interview to phone her therapist for advice on how to answer specific interview questions.

Candidate brought large dog to interview.

Applicant refused to sit down and insisted on being interviewed standing up.

Candidate dozed off during interview

••••••••••••••••••••••••••••••

Nuggets of Wisdom to get you through the day – Ed.

Rome did not create a great empire by having meetings; they did it by killing all those who opposed them.

If you can stay calm, while all around you is in chaos ... then you haven't completely understood the seriousness of the situation.

Doing the job RIGHT the first time gets the job done. Doing the job WRONG fourteen times gives you job security.

Artificial intelligence is no match for Natural Stupidity.

A person who smiles in the face of adversity... probably has a scapegoat.

Plagiarism saves time.

If at first you don't succeed, try management.

Never put off until tomorrow what you can avoid altogether.

TEAMWORK... means never having to take all the blame yourself.

Never underestimate the power of very stupid people in large groups.

Hang in there, retirement is only thirty years away.

Go the extra mile. It makes your boss look like an incompetent slacker.

A snooze button is no substitute for no alarm clock at all.

When the going gets tough, the tough take a coffee break.

INDECISION is the key to FLEXIBILITY

Succeed in spite of management.

Aim low, Reach your goals, Avoid Disappointment

Never test the water with both feet.

It may be that your sole purpose in life is simply to serve as a warning to others.

No one is listening until you make a mistake.

Always remember you're unique, just like everyone else.

Experience is something you don't get until just after you need it.

A closed mouth gathers no foot.

Don't be irreplaceable; if you can't be replaced, you can't be promoted.

Good judgement comes from bad experience and a lot of that comes from bad judgement.

A pat on the back is only a few centimetres from a kick in the butt

Never argue with an idiot. They drag you down to their level and then beat you with experience.

Following the rules will not get the job done.

Getting the job done is no excuse for not following the rules.

If it wasn't for the last minute, nothing would get done.

On the keyboard of life, always keep one finger on the escape key.

If you are good you will be assigned all the work. If you are really good, you will get out of it.

When you don't know what to do, walk fast and look worried.

You can go anywhere you want if you look serious and carry a clipboard.

Never raise your hands to your kids. It leaves your groin unprotected.

I'm not into working out. My philosophy is "no pain, no pain".

I'm in shape. Round is a shape.

I've always wanted to be somebody, but I should have been more specific.

••••••••••••••••••••••••••••••

HUMOUR PAGES

No pun in ten did – Ed.

Two vultures board an aeroplane, each carrying two dead racoons. The stewardess looks at them and says, "I'm sorry, gentlemen, only one carrion allowed per passenger."

Two boll weevils grew up in South Carolina. One went to Hollywood and became a famous actor. The other stayed behind in the cotton fields and never amounted to much. The second one, naturally, became known as the lesser of two weevils.

Two Eskimos sitting in a kayak were chilly, but when they lit a fire in the craft, it sank, proving once again that you can't have your kayak and heat it, too.

A three-legged dog walks into a saloon in the Old West. He slides up to the bar and announces: "I'm looking for the man who shot my paw."

Did you hear about the Buddhist who refused Novocain during a root canal? He wanted to transcend dental medication.

A group of chess enthusiasts checked into a hotel and were standing in the lobby discussing their recent tournament victories. After about an hour, the manager came out of the office and asked them to disperse. "But why?", one asked, as they moved off. "Because," he said, "I can't stand chess nuts boasting in an open foyer."

A woman has twins and gives them up for adoption. One of them goes to a family in Egypt and is named "Ahmal." The other goes to a family in Spain; they name him "Juan." Years later, Juan sends a picture of himself to his birth mother. Upon receiving the picture she tells her husband that she wishes she also had a picture of Ahmal. Her husband responds, "They're twins! If you've seen Juan, you've seen Ahmal."

These friars were behind on their belfry payments, so they opened up a small florist shop to raise funds. Since everyone liked to buy flowers from the men of God, a rival florist across town thought the competition was unfair. He asked the good fathers to close down, but they would not. He went back and begged the friars to close. They ignored him. So, the rival florist hired Hugh MacTaggart, the roughest and most vicious thug in town to "persuade" them to close. Hugh beat up the friars and trashed their store, saying he'd be back if they didn't close up shop. Terrified, they did so, thereby proving that Hugh, and only Hugh, can prevent florist friars.

Mahatma Gandhi, as you know, walked barefoot most of the time, which produced an impressive set of calluses on his feet. He also ate very little, which made him rather frail and with his odd diet, he suffered from bad breath. This made him a ……. a super callused fragile mystic hexed by halitosis.

And finally, there was a man who sent ten different puns to friends, with the hope that at least one of the puns would make them laugh. Unfortunately, no pun in ten did.

FOR ALL OF YOU THAT WILL NEVER MAKE "WHO WANTS TO BE A MILLIONAIRE" OR EVEN "THE WEAKEST LINK"…. HERE'S THE WORLD'S EASIEST QUIZ!

Passing requires 4 correct answers!

1) How long did the Hundred Years War last?
2) Which country makes Panama hats?
3) From which animal do we get cat gut?
4) In which month do Russians celebrate the October Revolution?
5) What is a camel's hair brush made of?
6) The Canary Islands are named after what animal?
7) What was King George VI's first name?
8) What colour is a purple finch?
9) Where are Chinese gooseberries from?

All done?
Check your answers below.

ANSWERS TO THE QUIZ

1) 116 years
2) Ecuador
3) Sheep and Horses
4) November
5) Squirel fur
6) Dogs
7) Albert
8) Crimson
9) New Zealand

WHAT DO YOU MEAN YOU FAILED?

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	John Bevan	Audit & Computer Security Services	01992 582439 john_bevan@ntlworld.com
DEPUTY CHAIRMAN	Pete Biss	EMX Co Ltd	01279 858300 pete_biss@hotmail.com
SECRETARY	Siobhan Tracey	BFG plc	01494 442883 siobhan.tracey@booker.co.uk
TREASURER	Jan Lubbe	KPMG	020 7774 8303 Jan.Lubbe@gs.com
MEMBERSHIP SECRETARY	Celeste Rush		020 8858 7384 RushLSE97@aol.com
JOURNAL EDITOR	John Mitchell	LHS Business Control	01707 851454 john@lhscontrol.com
WEBMASTER	Allan Boardman	Goldman Sachs	07881 930814 webmaster@bcs-irma.org
SECURITY PANEL LIAISON	John Mitchell	LHS Business Control	01707 851454 john@lhscontrol.com
MEMBER SERVICES BOARD LIAISON	Celeste Rush		020 8858 7384 RushLSE97@aol.com
EVENTS	Siobhan Tracey	BFG plc	01494 442883 siobhan.tracey@booker.co.uk
	Alex Brewer	Lloyds TSB	020 7418 3544 alex_brewer@bigfoot.com
	Rosemary Mulley	NabarroNathanson	0118 950 5640 r.mulley@nabarro.com
ACADEMIC RELATIONS	David Chadwick	Greenwich University	020 8331 8509 d.r.chadwick@greenwich.ac.uk
LOCAL GOVERNMENT LIAISON	Peter Murray		01992 582105 cass@peterm.demon.co.uk

Membership Enquiries to:

Janet Cardell-Williams
49 Grangewood, Potters Bar, Herts EN6 1SL
t: 01707 852384
f: 01707 646275
e: members.irma@bcs.org.uk
www.bcs-irma.org