ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 4 NUMBER 3 WINTER 93/94

The British Computer Society

Members' Meetings for 1994

Tuesday 8 February	**Access control**	Dr Brian Collins PC Security Limited
Tuesday 22 February (Full Day)	**Discussion Group (Quality Issues)**	Kit Robson - BSI Gary Hardy - Touche Ross Jeff Ridley - South Bank University Brian Kervill-White - Business Accountancy Group
Tuesday 8 March	**Viruses**	Jan Hruska Sophos
Tuesday 12 April	**Annual Debate with the EDPAA**	TBA
Wednesday 11 May (Full Day)	**Annual Conference & AGM** (London Press Centre)	Outsourcing of I.T.

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

Details of discussions groups are forwarded directly to members as part of the quarterly mailing. Please contact Bill Barton on 071 872 6720, or Steve Pooley on 0580 891036, for further information.

For details of the annual conference please contact Paul Howitt on 0992 644250.

LETTERS TO THE EDITOR

are welcome, write to:
Rob Melville

Centre for Internal Auditing
City University Business School
Frobisher Crescent
Barbican Centre
LONDON EC2B 2NU

Editorial

One of the great benefits of computers is the sheer ease and power of communications. As regular readers of the Journal will know, electronic communications have enabled articles to be solicited, submitted and refereed. Electronic mail has been used to raise issues with journalists and academics from other continents. These are all tried and tested ways of speeding up existing systems; with 'snail mail' and fax machines much of our electronic communications could be duplicated. But with the electronic bulletin boards available from private and public suppliers available for subscribers to networks, an entirely new culture has been created. This is the world where 'netheads' (or, more disparagingly, 'spods') spend literally hours logging in to conferencing and bulletin systems to discuss literally any subject that can be thought of. And some that you probably could not, unless you were attracted to exotic and arcane subjects . . . For example, Network News, a subscription service available to anyone on the academic network has thousands of continuing debates, updated with contributions from all over the world every day. (You want to know about old computer equipment? Log in to 'alt.technology.obsolete'. The latest Michael Jackson jokes? Try 'alt.tasteless.jokes'. Even news from California was quicker across this network than by more formal media.) City University students and staff run a very popular BBS where one of the facilities is a 'talker', like a series of public and private rooms for users to chat. The downside of this is that I have seen students literally flirting with each other across the net *while in the same room* yet not actually approaching each other in real life. The more serious aspect is that users can share their thoughts and knowledge across the world.

Anyway, these examples serve only to introduce a plea for some support, suggestions and advice from the readership. It has been agreed in principle that a bulletin board service for auditors can be set up on a world wide network which already covers academic, computing and accounting matters. It is likely that there will be a separate section for computer audit. In order to set up the most useful service I would like to find out who would want to be involved in deciding which topics to cover, and also if any reader would like to help manage the service. It can almost certainly be done electronically via e-mail through me, so no time-consuming meetings will be necessary. Early ideas include specific audit issues such as operating systems, PC's, technology, best practice, news items, and a help forum. It would probably even be possible to put this journal on-line, as has IFIP with its bulletin. Please mail any ideas to me.

The response to Ed Hutt's refereed paper on fault tolerant audit was exceptionally good, with many enquiries and requests for copies. There is always room for such well written technical pieces, and any potential author can rely on supportive editing and advice from other committee members. It also helps our members by showing what can be done with the right knowledge. In future issues it is planned to include regular practical columns, beginning with a UNIX column. Other topics might include PC's, networks, FM, operating systems and developments. Please call me to discuss these, even if you can only submit small irregular pieces. It's a service to your colleagues and it looks good on the CV, and any advantage these days is surely welcome.

And a happy and prosperous New Year to you all.

ROB MELVILLE

The views expressed in the Journal are not necessarily shared by CASG. Articles are published without responsibility on the part of the publishers or authors for loss occasioned in any person acting, or refraining from action as a result of any view expressed therein.

EDP AUDIT
NATIONWIDE

SENIOR COMPUTER AUDITOR

West Midlands **To £25,000 + Bens**

This global engineering organisation currently requires an experienced Computer Auditor with a degree, a successful track record auditing multihardware environments and willing and able to travel up to 70% of the time worldwide.

COMPUTER AUDITOR

East Midlands **To £23,000**

This major utility with a highly successful team of Computer Auditors requires an additional team player to undertake pre/post implementation reviews, Systems Under Development audits, and extensive application reviews. This is an excellent career development opportunity.

COMPUTER AUDITOR

North East **To £25,000**

Our client, a leading international insurance company, requires a Computer Auditor with 2 years' experience reviewing systems under development on IBM mainframe platforms. You should preferably be QiCA or CISA qualified.

SOUTH WEST OPPORTUNITIES

Bristol/Swindon **To £25,000 + Bens**

Two major financial organisations expanding their Computer Audit functions are seeking to recruit experienced computer auditors with DP or accountancy backgrounds. Successful applicants will have carried out audits on one or more of the following platforms, IBM Mainframe, DEC VAX, Unix Platforms and PC LAN.

LAST ORDERS!!

Bedfordshire **To £30,000**

Our client, a leading international brewery with an expanding computer audit department, is currently recruiting for a young Qualified Chartered Accountant with at least 2 years' EDP Audit experience preferable with one of the big 6. The successful applicant should be able to demonstrate strong interpersonal and presentation skills. EXCELLENT CAREER PROSPECTS.

TECHNICAL AUDITOR

North West **To £28,000 + Bens**

This highly successful audit department of a leading financial institution is currently recruiting for an EDP Auditor with strong technical background in one or more of the following: Unix Platforms (pref. AIX or Ultrix), Local and Wide Area Networks and DEC VAX. Previous experience will have been gained in a technical DP role, i.e. systems programmer.

SENIOR COMPUTER AUDITOR

City/Far East **To £45,000 + Bens**

This is a first class opportunity for the very experienced Computer Auditor who wants to retain the hands on skills and at the same time enjoy total responsibility for a large geographical and business area covered by this leading Merchant Bank. Applicants should be able to demonstrate a successful track record in banking, EDP Audit and possess strong interpersonal skills.

CONSULTANCY

UK Wide **To £30,000**

Three of the major big 6 audit firms are offering excellent career paths to EDP auditors with either an accountancy or DP background. Applicants should have a minimum of 18 months' experience auditing a variety of systems, and track records in manufacturing, financial, or banking industries.

SYSTEMS DEVELOPMENT AUDITORS

North West **To £22,000 + Bens**

This leading finance house undergoing major expansion to its EDP audit team, is currently seeking to recruit systems professionals with a minimum of 18 months' EDP Audit experience. Excellent career opportunities will be on offer to the successful applicants. Either QiCA or CISA qualification would be beneficial.

TELECOMS

City Based **To £30,000 + Bens**

This world leader in the telecommunications market place is currently seeking to recruit a young qualified ACA with a big 6 background and at least 18 months' EDP Audit experience. International travel will be part of the job along with senior management and board level presentations.

HANDS ON AUDITS

City **To £40,000 + Bens**

This top American merchant bank requires a Computer Auditor with at least 5 years' experience to join their small team responsible for the European Operation. Hardware platforms include IBM Mainframe, DEC VAX, PCs and Unix based. The successful applicant will enjoy excellent career progression.

As from 21st February 1994
MBA's new address will be 1 WILLOW STREET, LONDON EC2

MBA

The first step towards your next career move should be to contact Sean Farrell on 071-454 9010 (till 5.30 pm) or 081-318 3785 evenings/ weekends. Send a full cv to
Michael Bailey Associates Ltd,
Rococo House, 281 City Road,
London EC1V 1LA
Fax: 071-490 3361

MBA

Contents

SUBMISSION DEADLINES

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

Chairman's Corner

John Mitchell

The service that we provide to our members is very important to those of us who sit on your Management Committee. This Journal is of particular importance, because for many of you it is your only link with us and other members. Over the years we have built-up a portfolio of discounts for you, but we have been a little lax in not reminding you of those that are currently available. In order to redress the situation we have created a new post on the Committee with the title of Member Services. Nigel Smith has generously offered to take up this role and he will using the Journal to keep you regularly informed of the various discounts and other services that are available to you.

On the subject of services, it is now some five years since we last tried to find out what services you would like. At that time we issued every member with a stamped addressed envelope in order to elicit a reply, but alas we can only assume that the majority of you steamed off the stamp as we only received some forty replies from a total population of about three hundred at the time! We intend to repeat the exercise, but this time via the Journal and without a stamped envelope, so this will be a real test of your responsiveness. Remember, this is your group, but we need your help to make sure that it meets your requirements. Keep your eyes peeled for the survey form in the next issue.

The BCS is piloting a scheme for Continuous Professional Development and we were asked for our views on the subject. We, your Committee that is, tend to support the idea in principal, but have reservations about the way it would work in practice. The BCS appears to be thinking along the lines of a very formal process of accreditation of training courses and the like, but we would like a less formal self-assessment process, as is the case with other professional bodies such as the EDPAA and the ICAEW, where relevant reading, article writing, lecture preparation and the like is acceptable. The jury is still out on this one, but at least we were asked for our views. What about you? If you would like to let us know your views on this, or any other matter, then simply drop a line to the editor. This is after all, your Journal.

Have you heard the one about the 24 hour help line? Well Central Point Software claim to have one, but it was closed between 24th December and the 4th January. I suspect it closes for all the public holidays, which makes it availability factor about 95%. Some 24 hour service! Do you have any similar contradiction in terms to share with us? If you do, then please write to Rob Melville for inclusion in future editions. Why should computer audit be dull and boring? Answers on that one also to Rob please!

Guidelines for Potential Authors

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

An invited article need not be technical or overly academic (even Computer Auditors have a sense of humour!). In fact it need not even be 'invited'. Submission without invitation is encouraged and although this may lead to severe sub-editing by the Editor, submission will virtually guarantee publication.

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

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

Insuring Computer Related Risks - A Challenge for the 90's

by David Davies ACII,
Executive Director, Hogg Risk Managers.

David joined Hogg Group in 1967, and has executive responsibility for Hogg Risk Managers and Brokers' Research, Marketing and Communications functions.

David is recognised internationally as a leading author and speaker on risk management and insurance subjects. He has chaired seminars on risk and insurance issues in Australia, Malaysia, Bahrain and Europe, and currently leads the Insurance Institute of London's advanced study group into computer crime. Between 1985 and 1991 he was Risk Management Editor of the Computer Law and Security Report.

Overview

There are very few companies that get their computer insurance right. The blame for this can be apportioned almost equally amongst the buyers, the insurers and the intermediaries.

The way out of the log jam is to improve the buyer's ability to identify the cover that they need, and reject the very sub-standard policy wordings and approaches that are being offered by much of the insurance industry. Improvements will only come this way round - recent history has shown that when the insurance industry offers policies that are more appropriate to the buyer's needs, but that when those needs are not appreciated by the buyer, the effort and investment the insurer has devoted to the new initiative is wasted through lack of sales.

The key to buyer education is to build a bridge between the individual responsible for insurance within the organisation (usually the insurance officer or company secretary) and the information technology manager or director. In most organisations these two individuals rarely confer, do not understand each other's language and treat each other on a need to know basis. It is the building of this bridge that could be the opportunity for auditors (internal or external) to achieve great things.

This article will address five topics:

- why companies insure
- the strategic approach that they should take
- the impediments to that approach
- evidence taken from policy wordings, proposal forms and marketing statements
- a recommended strategy to take account of the shortcomings in the computer insurance market.

Why insure

The wrong reasons:

Blind faith -many insurance buyers have the perception that insurance will solve all of their problems. As will be seen later, this perception is often encouraged by the insurance companies' marketing departments. The buyers rarely read their policies, particularly the fine print, until they have a claim.

To avoid other action - many companies view insurance as an alternative or an excuse for not taking other risk management measures. "We do not need a contingency plan, we are fully insured". As will be seen, insurance is a useful component of a risk management strategy, but should never be used as a sole alternative.

The sheep instinct - when discussing new insurance covers, a common reaction is "what do other companies do?" The insurance buyer wants to make sure that they are above criticism by not doing any less than their opposite number in other organisations.

The good salesman - many insurance policies have been sold by good salesman who are quite capable of selling refrigerators to Eskimos, let alone unnecessary insurance to corporate buyers.

The January sales - there are periods when insurance is a particularly good buy (the soft market cycle) and, just like the shopper attracted by knock down prices in the sales, insurances are bought because they are cheap at that time, regardless of whether they are really needed.

There is only one valid reason for buying insurance and that is that it is part of a strategic risk management approach.

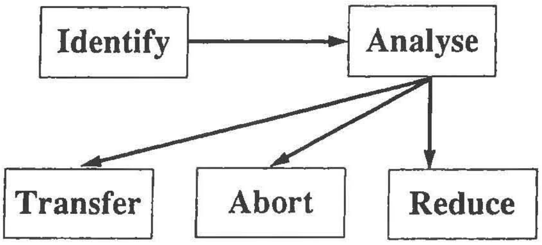
The Strategic Approach

The risk management process can be represented by a flow chart (Figure 1) from which it will be seen that:

- The core of the process is the decision as to the strategy that is to be adopted.

- That decision process must be preceded by an identification and analysis of the risks that are faced by the organisation, and by an understanding of the strengths and weaknesses of the available risk management processes.

The Risk Management Process



Risk Management Workshop

Figure 1

It should be extremely rare for a single risk management process to be adopted as the "solution". The strategy will normally dictate a balance of elements, each working to its own cost effective level, bearing in mind the uses of the other components within the strategy. i.e. A simple strategy might be:

- Self insure all risks up to £N. This will have the advantage of cost effective use of the insurance market (there is no merit in swapping pound notes with insurers for regularly recurring losses); in addition, it will provide an incentive (risk ownership) to the trading companies or business units within the organisation.

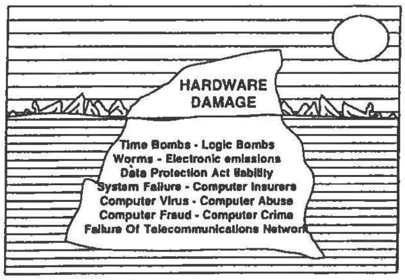
- Utilise resource (primarily management resource - training, management controls and motivation techniques) to reduce risks using the 80/20 rule.

- Develop contingency plans for obvious foreseeable catastrophies.

- Use insurance as a catastrophe safety net for major exposures and remoter but catastrophic risks. Find an insurer that will recognise the quality of the risk management controls by realistic premium rate reductions.

The first process of risk identification is particularly critical for computer risks. The insurance industry, and many buyers, have not yet appreciated that, whereas in the 1970's when computer policies were first developed, the dominant feature of computer risk was the value of the hardware, that risk is today comparatively insignificant - however, the much reduced hardware value is only the tip of the iceberg, with much beneath the surface of the water. Only a covert risk audit will reveal to what additional risks the company is exposed (Figurc 2).

I.T. Risks - The 90's


HARDWARE DAMAGE
Time Bombs - Logic Bombs
Worms - Electronic emissions
Data Protection Act liability
System Failure - Computer Insurers
Computer Virus - Computer Abuse
Computer Fraud - Computer Crime
Failure Of Telecommunications Network

Risk Management Workshop

Figure 2

Impediments

Each of the role players that has an influence in the quality of computer insurance, is disadvantaged in a number of areas:

The buyer:

The insurance buyer rarely understands the risks to which their organisation is exposed because of its use of information technology. The buyer is used to insuring physical assets and has great difficulty relating to the possibilities of logic bombs, hackers, third party fraud, network failure etc. It is rare for the person responsible for insurance buying to be computer literate or to understand either the language or the technology.

There is often a gulf between the insurance buyer and the DP or IT manager. To quote the insurance buyer for a major internationally known organisation "the first that I heard of our new computer systems was when I saw a photograph of the new hardware in the staff magazine".

The DP or IT Manager:

The DP or IT manager is rarely consulted on the insurance strategy. They do not understand insurance and in any event, their perception is limited to the data processing function - they are not able to perceive the impact of the non-availability of computing services on the user departments or the impact on the organisation that would flow from the mis-use or abuse of computer systems or data.

The bridge between the insurance buyer and the insurer is often the insurance broker. However, most brokers merely sell what is available and, understandably, only develop new initiatives in response to buyers needs. However, as we have seen the buyer rarely appreciates their own needs so demands little new from the insurance market.

The Insurer:

Most Underwriters have absolute faith in insurance as a solution to their policyholder's risks, rarely understand computing or computing language and may respond in an emotive way without fully understanding or studying the nature of the threat and its relevance to the cover they are giving.

Even when insurer wishes to take an innovative approach, they are limited by the structural divisions within the insurance market (the re-insurance that is so necessary if they are to insure catastrophe risks). The structural limitations straight jacket them into the traditional approach to computer risks, which is that the majority of risk is insured within the engineering departments of insurance companies because when the first computer policies were developed, they were pieces of mechanical plant that punched holes in cards, often suffered from mechanical breakdown and were sited within their own environment (fortress mainframe).

Insurers also find it very difficult to differentiate between good quality risks and those of low quality. They are happy with absolutes (a computer installation does or does not have fire extinguishing devices) but are unable to make a judgement on the quality of a business continuity plan or the management systems designed to control and motivate the users.

Evidence

The first piece of evidence is the structure of the policies that are used by virtually all insurers. Outside the financial sector, virtually all specific cover is provided by two policies, the 'Computer Policy' and the 'Fidelity Guarantee' or 'Crime Bond'. The Fidelity Guarantee policy has been available for half a century and today's 'Computer Policy' is very similar to the first computer policies of two decades ago.

Even with the better versions of these two policies, companies will only be insured for:

- fraud by employees
- loss or damage to hardware
- loss or corruption of data (but probably only for re-keying costs - see 'the six most common mistakes' below)
- lost profit or increased costs following material damage or failure of power or telecommunications.

Some of the above cover may be shared with wider non-computer specific policies (general material damage and general consequential loss following damage).

They will not be covered for events such as:

- logic bombs causing system failure
- computer extortion
- the cost of verifying the integrity of data following third party intrusion
- computer espionage

In short, the rule of thumb is: if it is risk that has been around for a long time, it is probably insurable; if it is a risk that has come into its own in its last decade, it is probably uninsurable.

The second piece of evidence to support these dramatic statements is the six most common mistakes that organisations make when trying to insure their computing risk. These are:

Data:

1. The sum insured usually assumes that all backups are intact and relates only to the cost of re-keying work done since the last off-site backup was taken. In reality this comparatively minor risk should be self-insured; the true purpose of insurance is to provide financial compensation in respect of the more remote but potentially catastrophic events. It is perfectly possible for a company to lose all data and there are many instances of this in the public domain and even more known only to the victims companies and their consultants.

2. Cover is usually limited to the costs of "re-keying" data - this wording and assumption dates back to the days when the data prep department keyed information into the computer from forms that were then retained and could be re-accessed. It takes no account of modern trading conditions under which data is entered as it is collected with no hard copy record.

Consequential loss:

3. Many companies still insure for the increased costs of working on the assumption that, if they have a disaster, they will be able to recover without losing profit. In reality, most companies would lose profit within a very short time of losing their computing functions and without a properly tried, tested and rehearsed business continuity plan, will not be able to recover for several weeks, if not months.

4. Where profits cover is selected, optimistic sums insured are chosen, on the assumption that recovery will be speedy and easy. Again, numerous case studies have shown that this is rarely the case.

Fraud:

5. Those companies that do insure against fraud (fidelity guarantee or crime bond covers) usually insure only against fraud by employees, not by third parties who may be able to access the computer systems.

6. Despite the fact that fraud insurance is based on a warranty that all of the systems of check and supervision disclosed to insurers are fully operative, few companies keep pace with the dynamic changes that are now happening within organisations, by continually reviewing the information that has been disclosed to insurers and advising them of every material change.

It is also rare for every aspect of the systems of check and supervision declared to insurers to be fully operative at all times. Under such circumstances Insurers, have the right to decline claims, and often do - more than 50% of fidelity guarantee claims fail for this reason.

The third piece of evidence is the advertising used by insurers to project the image of insurance as the total answer to risk. In one campaign an insurer illustrated, by a series of cartoons, a story in which a data processing manager confided to his managing director his fears that the company had become totally reliant upon its computers. The managing director (who was shown smoking a pipe in the computer room) had a single answer to those fears - he phoned his insurance broker and arranged a computer policy. We were then shown a computer disaster, which looked like a very explosive type of head crash. The disaster frame was the penultimate; in the final frame the DPM poked his head through the managing director's door to tell him "The computer's up and running and the records will be back on file by the end of the week". The managing director, who was shown grinning and reading his computer policy, responded by saying "Thank goodness for (the name of the insurance policy)".

Many insurance companies and brokers still have this perception about how easy it is to recover from a computer disaster and how complete is the "solution" that insurance is capable of.

The fourth piece of evidence is the questions that appear on proposals forms, particularly for Fidelity Guarantee cover. It is important that insurers get their proposals forms right because the insured has an absolute duty of disclosure and the proposal form should assist the insured by prompting them to tell them about all the facts that are material to the risk in question. However, an examination of many proposal forms shows how limited insurers understanding of computer risks really is.

There are three categories of questions that can be spotted almost immediately -

1. Questions that were designed for fortress mainframe technology of the 1970's, for example

"Who has access to the computer operations room

(i) during shift hours

(ii) outside shift hours"

2. Questions that skate the surface - looking for yes/no answers when the information that will be obtained by a positive answer is almost worthless. For example:

"Have you a database security system?

Does it cover disks and tapes?

Is it fully implemented"?

3. Questions that use computer buzz words that the insurer does not really understand, that may be capable of many interpretations but that were included "to show that we were into computer risks". Example:

"Is modular programming employed?"

The reason why insurers, who are themselves massive computer users, do not take more time and care with their computer related proposal forms can be summed up in the answer given by one underwriter when asked that very question:

"We spent two days with our DP people trying to draft a new proposal form. We could not really understand what they told us, so in the end we kept the form we were familiar with."

The fourth group of evidence relates to the words used by Insurers in their policy documents. Again, these can be grouped into a number of categories:

Cover for 1970's technology:

"Electronic data processing media means **the punched cards, punched tapes** or magnetic disks or other bulk media on which electronic data are recorded"

- incredibly this is from a 1991 policy that was heralded as state of the art.

No understanding of even basic computer terminology:

".... damage ... to data contained on data carrying materials **or programs** ..."

- this 1988 wording indicates that underwriters believe that programmes are some sort of a variation on disks and tapes.

Viewing the computer as mechanical plant:

"(Cover excludes) loss or damage to bulbs, valves, tubes, ribbons, fuses, sears, belts, wires, chains, rubber tyres, exchangeable tools, engraved cylinders, objectives made of glass, porcelain or ceramics, sieves or fabrics or **any operating media (e.g. lubrication oil, fuel, chemicals)"**

- this "material damage low voltage wording" is the standard vehicle for insuring German computer risks in the 1990's.

Limited data cover:

"In case of loss of, or damage to electronic data processing media ..., underwriters shall only be liable ... for not more than the cost of the blank media, plus the cost of labour for the actual transcription or copying of data, which shall have been furnished by the insured, in order to reproduce such electronic data processing media ... only if such items are actually reproduced by other electronic data processing media of the same kind or quality ..."

- this clause, again from a 1991 "state of the art" computer crime wording, is open to many interpretations as to what on earth the underwriter is trying to get at, but is probably meant to limit cover to the cost of making a tape-to-tape copy, not even re-keying costs.

Shooting cover in the foot:

"Computer virus means a set of unauthorised instructions, programmatic or otherwise, that propagate themselves through the Insured's computer system and/ or networks which instructions were **maliciously introduced** by a person other than an identifiable employee."

- the launch of this policy in 1991 was accompanied by much trumpeting of the fact that computer virus was included. However, computer viruses may be written maliciously but are rarely maliciously introduced. By their very nature, they are usually introduced accidentally under which circumstances cover is entirely negated.

The final piece of evidence is the policy conditions used by insurers; again, these demonstrate their considerable lack of understanding of computer risks.

"It is unwarranted that data is not stored for a longer period than the makers instructions"

- I call this the yoghurt clause.

"It is warranted that the insured has an archival filing system"

- this wording was used in a policy that was subject to a full on-site in-depth survey by a paid risk consultant. It would have been far preferable for the consultant to have examined and, if necessary, made recommendations on the methods used by the insured to archive data rather than include this somewhat bland warranty, violation of which will invalidate any sort of claim under the policy

"It is warranted that all equipment covered by this policy is the subject of a maintenance agreement .... which shall include provision for preventative maintenance"

- this may seem a reasonable requirement where insurers are providing cover for the consequences of breakdown, but most computer schedules include miscellaneous equipment - small printers, etc. that may not be the subject of a maintenance agreement. With this warranty on the policy, all cover is invalidated as the warranty applies to all of the equipment covered by the policy.

"Cover is conditional upon the insured not violating software licensing conditions"

- by their own admittance this warranty was introduced by an insurer that had gained the impression that viruses were spreading solely because of the practice of software piracy. With this clause on its policy, the insurer feels content.

The Strategy

Bearing in mind all the pitfalls that have been identified above there are a number of vital steps that are necessary in order to ensure that your organisation (or your clients' organisations) are not one of those that discover the limitations in their computer cover only when they have a major claim. Someone must be motivated to do the following:

1. **Identify the risks.** If necessary bring in outside consultants to undertake a covert risk analysis. Examine the impact of the loss the major threats to which you are exposed on the individual business functions that rely upon or use Information Technology within the organisation.

2. **Do not confine the studies to traditional computer risks.** Bear in mind the organisation's possible reliance on telephone systems, fax machines and the like. Include them in your studies and include them in your computer insurance specification.

3. **Put insurance in its place.** Use insurance as a safety net, not as an excuse for doing nothing else.

4. **Find two partners** - work closely with the data processing staff within the organisation and, externally, find an Insurer or Broker that is not hide bound by the traditions and limitations of the past.

5. **Treat any proposal forms or survey reports submitted to Insurers like dynamite.** Make sure

that the information fully represents the state of the risk, that all material facts have been disclosed and continually revise the information given to Insurers to make sure that it remains accurate.

6. **Read every word of the policy.** If Insurers' intentions are unclear ask for a comprehensive written explanation. Insist on this; switch Insurers if you cannot get it.

7. **Do not accept garbage.** You have the right to expect better.

8. Apply the golden rule of risk management - **never, never assume.**

The role of the auditor

The auditor can become the bridge, or catalyst, between those two empires of DP and insurance:

- Question, persuade, convince, recommend. Above all, attack the fog of complacency that surrounds the subject.

- Encourage the data processing or Information Technology Manager to consider the risks to which the organisation is vulnerable. Use of recommended impartial investigation techniques to deflate false assumptions.

- Carry the message to the Insurance Manager or Company Secretary or better still arrange a three way meeting.

- Compare the IT risk profile with the current insurance policies. Examine them in detail. Identify the pitfalls.

- Encourage the Insurance Manager to search out the Brokers or Insurers that can provide an intelligent response and that are prepared to consider the cover that you need.

In short, do not accept 1970's computer hardware policies to cover 1990's Information Technology Risks.

Myths about EDI - Accounting and Auditing

William List CA FBCS
Director, The Kingswell Partnership

He is the finance director of The Kingswell Partnership; a consultancy specialising in all aspects of business risk limitation. He is an acknowledged expert in the use of control and security techniques in application systems, including those involving networks, EDI and distributed processing. He is a member of the management committee of the EDI Accountants special interest group and Secretary of the BCS Security Committee.

The movement of information between organisations electronically has been a reality for many years. To achieve this movement the organisations agreed amongst themselves (or between them) exactly what form and format the information would take so that the computers processing the information could understand it. Initially the transfers were by magnetic tapes (Eg BACS) and more recently by transmission (Eg SWIFT).

As more and more organisations sought to gain the benefits of Electronic Document Interchange (EDI) a number of public standards setting out the form and format for commercial transactions (Eg invoices, orders etc) were developed. Today there is wide use of EDI in many commercial sectors (Eg retail) and organisations are seeking to increase its use.

The development has been largely driven by the technical staff, with user assistance in defining the contents of messages. Many people view it simply as a means to get information from A to B by computer, controlled by the technical staff.

With the exception of the imposition of certain access and authentication procedures EDI has, as yet, had little impact on the majority of business procedures. In fact many users print out all the messages and process them as if they were paper transactions.

In reality the use of EDI will, over time, cause major changes to clerical procedures in an organisation causing changes to work loads, work flows, internal control procedures and audit procedures. These changes are caused by the removal of paper from the processing and the consequent reduction in staff to handle the paper.

This article seeks to dispel certain current misconceptions about EDI.

EDI is a "magic" business improver

EDI is only a means of communication. Certainly faster and perhaps more accurate than paper methods. If there is less paper and error then perhaps less cost is incurred in processing it.

EDI used imaginatively often provides competitive advantage and possibly reduced stockholdings.

It may be very good for the business if the reason for using EDI is sound commercially and the system is implemented well and integrated into the business process.

EDI is "secure"

No transmission system is 100% secure - the Prime Minister proved this in the Summer. However well the PTTs, TTPs or VADS perform there remains a risk of loss of confidentiality and hacking - even if it is less than 1%. It is important therefore to ensure that appropriate controls are in place within your business to limit any likelihood of damage should the security in transmission fail.

EDI is legally insecure

As the majority of legislation was drafted assuming written documents and no case law covering EDI presently exists in UK. The exact legal position on Electronic documents is unsure. In practice however:

- it is possible to put a clause into an interchange agreement to state that both parties will accept them if a dispute arises and the civil court will accept this.
- the courts do take cognisance of commercial reality and appear to take a reasonable view of computer evidence.

Whilst the doubts remain in practice many large organisations use EDI to benefit their business without incurring undesirable legal side effects.

EDI is purely technical

This is true. The mechanisms for transmitting and receiving messages in standard formats and delivering them to or from application programs are purely technical.

Extensive use of EDI however causes material changes in the way business operates and the procedures within businesses. Records are electronic and fewer staff are needed to deal with them.

As a consequence there is need to revise internal control procedures to ensure that a constant (or improved) quality of control is achieved when transactions are not printed out.

EDI reduces audit problems

The effect of EDI is to replace paper as the means of recording transactions therefore changing the nature of the basic audit evidence. In addition there is often greater integration of business computer systems, giving rise to greater complexity.

The consequence for auditors is that:

- There will increasingly be the need to examine electronic transactions electronically as part of the normal procedures, and

- Audit staff will be required to evaluate the total system including some complex computer components in order to form a view on the quality of internal control.

These two consequences will cause change to the audit process but whether they reduce audit problems is hard to determine.

Auditors require paper records from EDI systems

This is not true. All competent auditors should be able to use automated tools to examine transactions electronically.

There are however requirements by HM Customs and Excise that limited paper output must be available for the VAT inspectorate.

Auditors may also be concerned that paperless systems are unable to be controlled They can be effectively controlled if the the technical and clerical procedures are designed as a whole and operate effectively. By performing a critical systems review any weaknesses in control can be identified and audit procedures modified accordingly.

EDI packages which include an audit module automatically satisfy audit and control requirements

Often all the "audit" module does is to create log files of transactions (and often not all of them). The requirements for control and security will be derived from a risk analysis relating to the applications using EDI. Audit requirements should be identified by the internal and external auditors.

Audit trails are only for auditors

This is a misnomer; Audit trails are logs of transactions or specific events. These are the primary tool for management to monitor the effectiveness of the system on a day to day basis. A secondary purpose is to be available for use should there be need to discover what happened in the system either to rectify a fault or investigate an incident.

Overall it seems that many of these misconceptions may have arisen because of a lack of understanding by management, technologists and auditors.

The Accounting Interest Group of the EDI Association is addressing the need to promote greater understanding outside the technical teams involved in EDI. We hope that our efforts will contribute significantly to realising the benefits of EDI in organisations.

If you wish further information on the EDI Association and the Accounting Interest Group please contact:

Mr Gary Lynch
EDI Association Secretariat
148 Buckingham Palace Road
London SE1W 9TR
Tel: 071 824 8848
Fax: 071 824 8114

Computer Auditors Don't Need Help

Nigel Smith

Nigel has twenty five years' IT and audit experience and has worked in the petrochemicals, oil, finance and automotive industries before starting his own consultancy practice in 1991.

An Honours Degree in Business Studies and completion of an MBA course have recently been supplemented by passing the TickIT auditors' course and examination.

Nigel is responsible for the recently created ***Member Services*** *which has been established to help the group's members by maintaining information on publication, courses and discounts on services, facilitate the interchange of information between members as well as the traditional function of maintaining the group's book stock.*

Computer auditors are professionals who have a wealth of IT experience as well as auditing experience and therefore are able to effectively audit anything IT related, system or hardware.

Whether or not you agree with the above statement (and I do not) I hope you would agree that we all benefit from sharing in other people's experiences.

A number of books have been written over the years on the subject of computer audit and auditing of specific aspects, such as Malcolm Lindsey's AS400 Auditing Handbook. Unfortunately the latter are rare and, as one would expect, often become out-of-date very quickly as technology and techniques change.

I have recently taken over the CASG's book stock and list overleaf the titles currently in stock; all you have to do is write or call me to obtain your copy of any of the books.

But you have nothing of interest to me, I hear you say.

This is perhaps the point of this article. I am sure there is a wealth of experience among our readership which as professionals we would not object to sharing with others. During the course of your work you will have prepared hypotheses, tested them and drawn conclusions on the adequacy of the systems, environment and procedures. You may have encountered the unusual and unexpected and are also likely to have prepared guidelines for the next audit. There may not be enough to write a book on the subject, but there may well be enough when compiled with other people's experiences in that area, form an informed and informative insight into the audit of a particular system, hardware platform or environment.

I haven't got time to write about my work, I'm too busy.

We are all busy; the economic climate of the last two years or so has meant that we have to make sure that our audits are value for money. What I am hoping is that you will all take a little of your precious spare time to jot down those tips and observations which would be helpful to your fellow professionals.

Don't leave it until later or to someone else, put pen (or printer) to paper and send it to me. Who knows, you may well amaze yourself as to how much you know about a particular computer audit topic. Don't forget, the obvious to you may not be obvious to someone else.

I look forward to hearing from you.

Nigel J Smith
N J Associates Limited
7 Parkfields
Welwyn Garden City
Herts AL8 6EE

0707 334421

see overleaf. . . .

BCS - CASG AND OTHER ORGANISATIONS' PUBLICATIONS

Title	Cost £
Control & Audit of Minicomputer Systems	TBA
AS400 Auditing Handbook	15.25
Data Protection & Security Guide for Personal Computers	TBA
Security & Control of Databases	TBA
Buying Payroll Software	n/c
Buying Stock Control Software	n/c
Buying Sales Order Processing Software	n/c

All prices quoted above are inclusive of postage and packing. For no charge publications, a donation (to cover postage and packing at least) would be appreciated.

Services

Library and information services at the IEE/BCS library:

Lending & reference services
Photocopy & document supply services
Technical information services
Courses information
Current and archive BCS activities and news

Further information from:

Ginny Bennett
BCS Librarian
Institution of Electrical Engineers
2 Savoy Place
London WC2 0BL
Tel: 071 240 1871 ext 310
Fax: 071 498 3557

Discounts

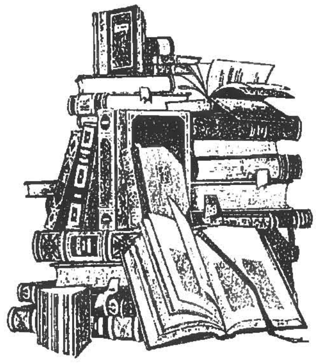
Publication	Discount
NCC Blackwell EDI Publications	7.5%
Computer Fraud and Security Bulletin	20%
Computers and Security	20%
Quality Software Report newsletter	25%

Other publications and discounts are being pursued . . . watch this space!

Contact Nigel Smith on **0707 334421** for more information on the discounts or services, or to obtain copies of the publications listed.

BOOK REVIEW

GOVERNMENT INFORMATION SYSTEMS AUDIT MANUAL



IIM Treasury, 1993
ISBN 0 11 560051 5
£20

This manual has in many ways been a long time coming. Its companion volume, the *Government Internal Audit Manual* has existed for a decade or so, and was updated in 1988. In the interim period, Government auditors were directed towards the CIPFA *Computer Audit Guidelines;* the publication of this book now supersedes that advice. The CIPFA *Guidelines* also have a venerable history, but have changed from 'how to' recipes for specific systems to a more general textbook. *GISAM* is also oriented towards high level, policy statement and best practice.

Now I have to say that both *GIAM* and the *Guidelines* have been part of my essential reference books for the last decade, and the new *GISAM* has been eagerly awaited. It's a good price for such a manual and is reasonably clearly written. Much of the content is sound advice, especially the strong recommendation that the systems approach is the most effective. Even the term 'Computer Auditor' is eschewed in favour of the more accurate 'Information Systems Auditor. But my initial feeling on reviewing *GISAM* was disappointment. While there may be strong arguments for government audit departments requiring a great deal more advice on policy, it is not good enough to concentrate on this alone at the expense of practical advice. For example, Section D describes 'Evaluate and Test', an area where many newcomers to computer/Information Systems audit need advice. They deserve better than a bland statement like 3.8:

> 'When devising a testing strategy the auditor will focus on the controls which are the most important to the attainment of system objectives and therefore, ultimately, departmental objectives. Tests should be designed to obtain evidence that critical controls operate effectively. The exact nature of tests to be applied should be determined by the audit manager and are not listed in this manual.'

But what if the audit manager is new to this type of audit? Or whose knowledge was gained in the large mainframe systems of the 1970's and 80's? It really does not help the auditor on the ground floor to know that the controls eventually link to department objectives. In fairness, the reader is prompted to look at Section G for possible procedures but this section is barely two pages long and so nebulous that it is of little use.

My other major criticism is the Bibliography of 'relevant Publications'. Of twenty publications, eleven are five years old or more, and one dates from 1970! The most common texts – Chambers and Court, Jenkins Cook and Quest, and Weber – are not mentioned. Neither are the EDPAA's 'Control Objectives' or any Institute of Internal Auditors or CASG publications.

In its favour, *GISAM* is available on diskette for purchasers and would provide a framework for audit departments new to this work. But for technical and practical guidance stick to CIPFA for the time being. There is a gaping hole in the market which used to be filled by CIPFA and Chambers. Unfortunately *GISAM* does not fill it.

EDPAA UNIX SPECIAL INTEREST GROUP TRAINING DAY

26th April, 1994 - Central London

The group are planning a Unix auditing training day which will cost approximately £50.
Interested parties should contact Chris Bunton on 071 836 7744
or Malcolm Lindsey on 081 710 7327.

casg

Management Committee

CHAIRMAN	John Mitchell	Little Heath Services	0707 654040
SECRETARY	Raghu Iyer	KPMG Peat Marwick McLintock	071 236 8000
TREASURER	Fred Thomas	Retired Consultant	0371 875457
MEMBERSHIP SECRETARY	Jacqui Race	The Stock Exchange	071 797 3551
PUBLICATIONS	Nigel Smith	NJ Associates	0707 334421
MONTHLY MEETINGS	John Bevan	Audit and Computer Security Services	0992 582439
	Alison Webb	Independent Consultant	0223 461316
CONFERENCE ORGANISER	Paul Howitt	Tesco Stores Ltd	0992 644250
DISCUSSION GROUPS	Bill Barton	The Rank Organisation plc	071 872 6720
	Steve Pooley	Independent Consultant	0580 891036
MARKETING & PR	Jarlath Bracken	Zurich Insurance	0705 853019
JOURNAL EDITOR	Rob Melville	City University Business School	071 477 8646 SC355@CITY.AC.UK

casg
Computer Audit Specialist Group

The British Computer Society

Membership Application/Renewal

(Renewals are due in August of each year)

PLEASE RETURN TO
Mr A J Thomas
Treasurer BCS CASG

3 Kings Court
The Maltings
Great Dunmow
Essex CM6 1UX

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

CORPORATE MEMBERSHIP (Up to 5 delegates)* * Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal and attendance at our meetings (see over)	£75
INDIVIDUAL MEMBERSHIP (NOT a member of the BCS)	£25
INDIVIDUAL MEMBERSHIP (A member of the BCS) BCS membership number: ____________________	£15
STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment). Educational Establishment: ____________________	£10

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

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

SIGNATURE: DATE:

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

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

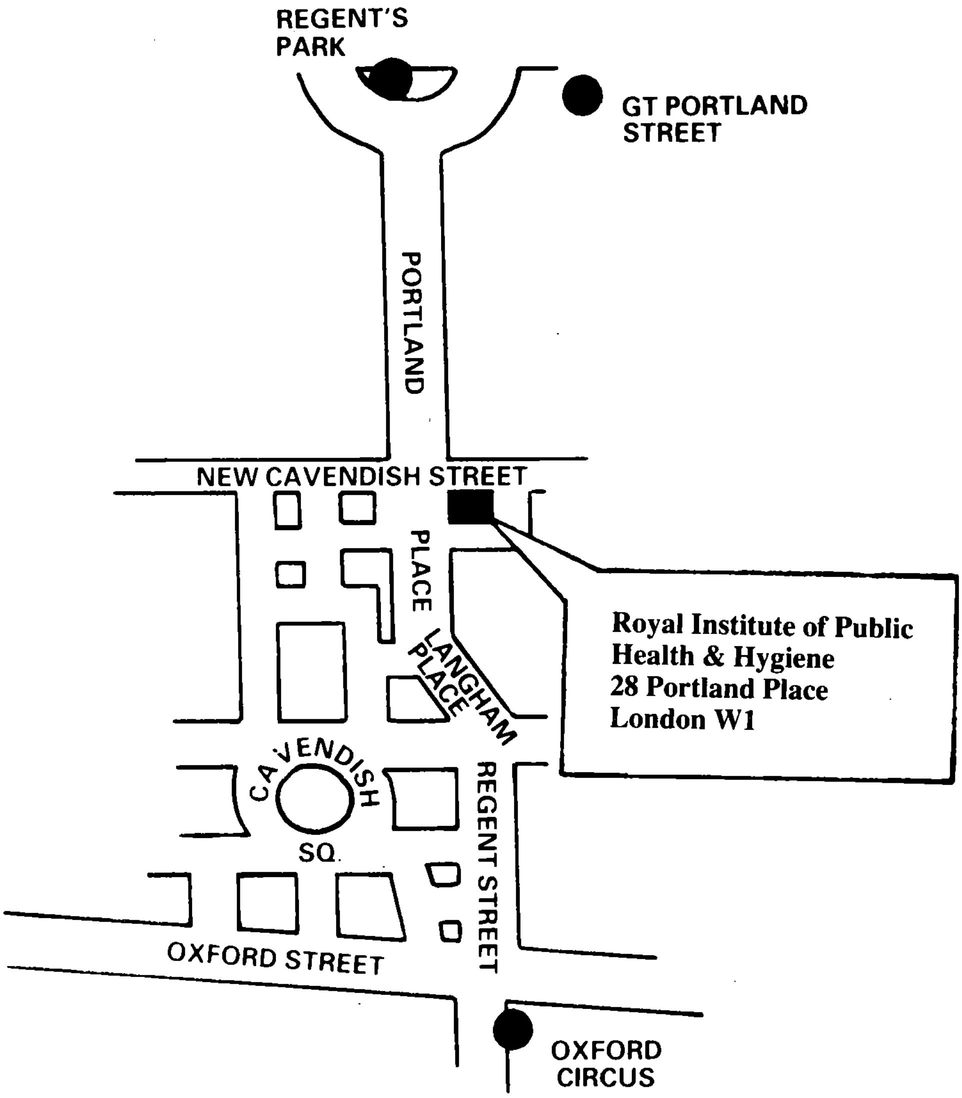
ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify

Venue for Members' Meetings



Printed by City University Print Unit