casg Computer Audit Specialist Group
JOURNAL
ISSN 0961-9348
VOLUME 7 NUMBER 3 SPRING 97
The British Computer Society

Technical Briefings 1996/97

8 October 1996
Auditing and automation

To be held jointly with the IT faculty of the ICAEW at their premises in Moorgate Place

Chairman	Paul Williams: Partner, Binder Hamlyn
Automating UNIX Audits	Mike Chorley, Trillion Software
Viruses from the Internet	Joseph Richardson, Dr Solomons
Data Matching	Simon Keane, London Team Against Fraud
Implementing automated working papers	Ken Ebbage, Pentana
Evaluating against BS7799 using COPIT	Andrew Birkbeck, Glynwedd Steel Ltd

---

Tuesday 14 January 1997
Networks: moving ahead securely

Royal Aeronautical Society

ATM and security	Leslie Hanson, Cabletron Systems Ltd
Open doors into networks	Rose Hines, IT Vulnerabilities
Moving to Novell 4: Security Implications	Peter Wood, First Base
Secure Gateway implementation	Yag Kanani. KPMG

Tuesday 15 April 1997
Systems development audit: Adding value

Royal Aeronautical Society

Diagnosing project problems, Signs and Symptoms Services	Ruth Woodhead, Admiral Management
Systems Development audit: The IS manager's view	Graham Folmer, Addenbrookes Hospital
Testing the Testers	Dorothy Graham, Grove Consultants
Preventing problem projects: the auditor's role at the outset	Geoffrey Smart, Coopers and Lybrand
Auditing RAD	Stan Dormer, Stan Dormer Associates

Followed by Annual General Meeting

Contents of the Journal

The ***Journal*** is the official publication of the Computer 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

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by Dodimead Ball, St Albans, Herts.

EDITORIAL

If every computer auditor were required, as part of their contract of employment, to write and submit one article a year for publication, then your editorial team would be snowed under with requests for publication. If the contract went one stage further and insisted that continued employment depended on publication, then the quality of those submissions would undoubtedly be very high. Unfortunately, I not only do not know of any contract with such a requirement, but I am personally aware of a number of organisations that positively discourage such interest from their staff. In some cases this is simply self protection: why risk a member of your staff getting credit for a good article when one's own is rejected? In other cases there is genuine concern that some confidential information may inadvertently enter the public domain. A concern that could be eliminated by letting the corporate lawyers loose on the thing prior to submission. This reminds me of a cartoon that I saw where the chairman is examining his corporation's Christmas card, "Season's Greetings! Looks okay to me, but we'd better run it past the legal department". Another reason is that you may think that you have nothing to add to the common body of knowledge: you would rather take from the work of others and not put anything back in. Now these various reasons for not doing anything are both laudable and base depending on your viewpoint, but in reality the reason that most people do not do things is sheer apathy. However, for every thousand of you who add nothing to the profession, there are one, or two who do more than their fair share. One such person is Alan Oliphant who has provided the main article for this edition. Alan is not just involved with the BCS. He is a great contributor to the IIA, where he sits on their Technology Committee and helps to organise COMPACS. He also provides input to ISACA and a number of Internet discussion groups. His article on the millennium problem is an example of someone who constantly puts back into the knowledge base far more than he takes out. An example, I hope, to the many of you who are feeling uncomfortable as you read this.

Now if your continued employment did require you to produce something, then I think that your organisation would benefit as well. After all, you all write well argued reports on how control in your company could be improved. Why not go one stage further and use that information to identify problems that may have a generic application? Other people would be doing similar things, so your company would benefit from them. The IIA motto is 'progress through sharing'. Please let us have a little more sharing and a little less taking.

I sometimes get involved in vetting membership applications to the Society. I used to be surprised when people would apply for membership and freely admit that they had done nothing to contribute to the profession in the last decade. Why do you want to join?, I would ask. The response, not unnaturally, was usually that the post nominal letters would help their career. When I query why they had not joined one of the many specialist groups, or not obtained any relevant qualifications, or had not spoken at any meeting, or not provided an article for publication, the responses are similar. They are not required to do so, why should they bother to do so? Apathy, once again and in those cases, no post nominal letters either, I'm afraid.

The job market may be buoyant at the moment, but most of us can remember the environment a few years ago. Next time, it may be you who gets pipped to the post by someone who has done that little extra. There are now more than 10,000 CISAs in the world, over 34,000 members of the BCS and 3,500 members of the IIA-UK. The three UK ISACA chapters number over 1,000 members between them. Your own CASG has about 400 members and the fact that you are reading this is a good sign. Why not stop reading and fire up that word processing package which is currently idling on your computer? Put something back in, even if it's only a letter to me. It may well be your salvation in the future when the chips are down.

John Mitchell

Chairman's Corner

Alison Webb

This issue gives me my first opportunity to welcome Jean Brown to the CASG. We have found that increasing numbers are coming to the Briefings, which of course is good for everyone: but the amount of organisation involved in staging them successfully is now quite significant, and the committee members involved were finding it quite a burden on top of their jobs and other commitments. Jean will be doing the bulk of the administration for our next Technical Briefing on 15 April, and we are very pleased that she has stepped in to help.

Perhaps this is also a good time to make a plea to members to help us simplify our administration, and thus keep the costs of Briefings as low as possible. We've long had a rule that we don't issue invoices, but in practice, kind-hearted committee members have bent the rules from time to time, because people who work for large organisations often find it difficult to get cash unless they go through their company's proper purchasing procedures.

Naturally, at a professional level we applaud the strength of your controls: but in some cases we spend almost the value of the final cheque in telephone calls and faxes to get it. Although everyone does their best, getting our invoices paid is one of the main time-wasters for the organisers. The day isn't managed by the same person and

therefore addressed the same place each time; some people go to CASG events and also events organised by other BCS specialist groups, and so on. There are countless muddles: and sometimes we never get our money.

We have asked Jean not to issue any more invoices: we don't want her to waste her time (and your money) collecting debts. So please, pay with a private cheque and claim the money back on expenses - don't try and turn us into unpaid (and sadly unsuccessful) credit controllers.

Finally, the last thing we want to do is to discourage anyone from coming to the Briefings: so if paying directly causes insuperable problems, please let me (personally) know, and we'll work out something to keep everyone happy, and all debts honoured.

BRIEF HISTORY OF THE WORLD - Part II

This follows on from the article in the last edition on the need for clarity of expression in our audit reports. The extracts are from genuine student bloopers collected by teachers throughout the United States, from eighth grade through college level. The spellings are exactly as used by the students - Ed.

Then came the Middle Ages. King Alfred conquered the Dames, King Arthur lived in the Age of Shivery, King Harold mustarded his troops before the Battle of Hastings, Joan of Arc was cannonized by Bernard Shaw, and victims of the Black Death grew boobs on their necks. Finally the Magna Carta provided that no free man should be hanged twice for the same offense. In Midevil times most of the people were alliterate. The greatest writer of the times was Chaucer, who wrote many poems and verses and also wrote literature. Another tale tells of William Tell, who shot an arrow through an apple while standing on his son's head.

The renaissance was an age in which more individuals felt the value of their human being. Martin Luther was nailed to the church door at Wittenburg for selling papal indulgences. He died a horrible death, being excommunicated by a bull. It was the painter Donatello's interest in the female nude that made him the father of the Renaissance. It was an age of great inventions and discoveries. Gutenburg invented the Bible. Sir Walter Raleigh is a historical figure because he invented cigarettes. Another important invention was the circulation of blood.

The government of England was a limited mockery. Henry VIII found walking difficult because he had an abbess on his knee. Queen Elizabeth was the "Virgin Queen". As a Queen she was a success. When Elizabeth exposed herself before her troops, they all shouted "hurrah". Then her navy went out and defeated the Spanish Armadillo.

The greatest writer of the Rennaissance was William Shakespear. Shakespear never made much money and is famous only because of his plays. He lived at Windsor with his merry wives, writing tragedies, comedies and errors. In one of Shakespear's famous plays, Hamlet rations out his situation by releiving himself in a long solioquy. In another, Lady Macbeth tries to convince Macbeth to kill the King by attacking his manhood. Romeo and Juliet are an example of a heroic couplet. Writing at the same time as Shakespear was Miguel Cervantes. He wrote Donkey Hote. The next great author was John Milton. Milton wrote Paradise Lost. Then his wife died and he wrote Paradise Regained.

During the Renaissance America began. Christopher Columbus was a great navigator who discovred America while cursing about the Atlantic. His ships were called the Nina, Pinta and the Santa Fe. Later the Pilgrims crossed the Ocean and this was known as the Pilgrims Progress. When they landed at Plymouth Rock, they were greeted by the Indians, who came down the hill rolling their war hoops before them. The Indian squabs carried porpoises on their back. Many of the Indian heroes were killed, along with their cabooses which proved very fatal to them. The winter of 1620 was a hard one for the settlers. Many people died and many babies were born. Captain John Smith was responsible for all this.

Tackling the Millennium Problem

Alan Oliphant

Introduction

On the 1st of January 2000, a considerable number of computer systems will fail to work correctly, resulting in confusion and potentially in business failure!

Why? Because the majority of computer systems cannot handle the change of date as we move from 1999 to 2000. This problem is by no means confined to the older mainframe legacy systems. There are many instances where similar problems have been introduced into some of the newer client/server applications.

This Briefing Note is intended to provide readers with some practical advice on what organisations should be doing to resolve the potential problems. It is by no means a definitive statement. The impact on individual organisations, even within the same sector, will be different.

It also needs to be stressed that a considerable amount of work will need to be done to resolve the problems. It will be expensive. There are no "miracle solutions". The only solution is hard work.

Finally, this can not be considered to be a definitive document. More potential problems emerge every day and it is impossible to provide a single solution to every organisation's problems. It should be looked at as a "snapshot in time". A starter document for those who have not yet begun the process and a checklist for those who have. Most computer systems store and refer to dates as a 6 digit number in the form ddmmyy. The year is referred to by the last 2 digits only. There is seldom any reference to the century.

Thus, when we move from 1999 to 2000, the year element of dates will change from "99" to "00". Thus, when calculations are performed using a two digit year code, the results will range from the misleading to the disastrous. Many systems will imply that the "true" year is 1900. This will have obvious effects on any processing which is date dependent or calculations where dates are involved. If you consider how much of your information processing depends on dates, the effect of this change will be apparent. It is not too paranoid to suggest that organisational failure could result.

This situation has arisen mainly because of historical limitations on storage capacity of computers. Valuable storage space was saved by not storing information about the century. It was easier to imply that a date was in the 20th century than to implicitly store the date as such. After all, when a lot of systems were written in the 60's, 70's and even 80's, no one really believed that the systems would still be running in 1999.

Sadly, there are a considerable number of these "legacy" systems still running. Even the "client-server" revolution has not replaced them all. In fact, there are a number of these applications which also do not allow for the change of century. It is very difficult to get out of bad programming habits!

This problem is not merely restricted to application systems which have been written in-house. It will also affect proprietary software, systems software and hardware.

If you fail to start the work in the near future, you will probably be too late. Remember, the delivery date is not 31st December 1999; it is most likely that your applications must be in place and working correctly by 31st December 1998 at the latest to allow for proper processing of future dates and to ensure that your accounting systems cope with the changes correctly in the last financial year before the change of century. In some businesses, future date processing will mean that changes have to be in place much earlier.

Remember that the year 2000 is also a leap year. How many times does this normally cause your business problems?

How many old programmers remember that they used to use the year 99 to signify an expiry date for a file or tape? These were potentially those files or tapes which were never to be purged during normal housekeeping. Look lively, the date of their destruction is at hand. Can you remember how many files or tapes are affected? You have them all documented of course; or have you?

The job is getting much bigger than many people thought it was.

And finally, this paper tends to concentrate on traditional computer systems. The problem also impacts any automation project. There has been speculation about the ability of the Global Positioning System to cope with a change of century (in fact some speculate that the system will fail sometime in 1997). What does this promise for air transport? Also, automatic building management systems are potentially built around processors which are not date compliant. I would not like to speculate on the impact of failure in these systems.

Summary

Solving the Year 2000 problems is not major "rocket science". It is a combination of common sense and, more importantly, very hard work. While there are a myriad of software products which promise to solve your problems overnight, the practices involved in the development of your "legacy" systems conspire to thwart any automated process.

The successful companies will be those which allocate resources early on and identify the significant problems. The really successful companies will be those who also commit to serious testing, to solid standards for the future and to eliminating the problems once and for all.

Common Approaches and Advice

The problem is a big one and resolution must be handled on a project basis. It is no different to any other major project. However this is one project which cannot be allowed to fail or to come in late.

If the project fails to deliver, there is a great probability that your business will also fail.

If the project does not deliver in time, there will probably be a similar impact on your business.

Business Involvement

Year 2000 work needs to be written into business plans to ensure that it gets the support and resource it needs.

It is critical that there is commitment from the Board of Directors and Senior Management to ensure that sufficient resources are available to carry out the work in time. Awareness campaigns early on in the project can help to raise support for the work from the business and ensure that a sufficient proportion of the annual budget is allocated to the work.

Company lawyers need to be briefed on the issues in the event that they need to put pressure on vendors who do not provide Year 2000 versions of their products.

After a "year 2000" project starts, the application programmers & systems analysts should meet with the users to explain what they can expect. The IS Dept. and the company need to plan to a make the year 2000 a top priority. Senior management and the users should be educated about the year 2000 by the IS Dept. and Internal Audit. Explain to them that the year 2000 project is a very high priority and other tasks will need to be moved aside. The programmers should attempt to wrap-up any pending tasks and to minimise the non-Year 2000 work-in-progress.

Planning

As with normal projects, the key to success is project planning. This is even more critical with Year 2000 changes, mainly because of the extent of the changes which are necessary and the impact of failure.

The Year 2000 projects can generally be broken down into:

- Impact analysis and portfolio sizing,
- Create a plan,
- Implementation of the plan (including the creation of test scripts, code conversion, and acceptance testing)
- Extensive system testing after the code changes are made.

The "test plans" and "acceptance tests" for each system to be converted can be over 80% completed while the "impact analysis" and "planning" (for implementation) phases are being conducted. The users should be fully aware of the huge Year 2000 resource allocation which will need to be made by the programmers.

Limit the production code changes which can be made while the source code is being made year 2000 compliant. This can only be done with users total involvement. However, you cannot put all changes on hold as some are needed for operational reasons (programs refuse to work) or for business reasons (new product launches).

At a minimum, the following elements need to be considered during the planning process.

What is the objective of the work?

Make sure that this objective is clearly communicated to the whole organisation and ensure that it has the full support of all management.

The objective of the work should be to ensure that all software, programs, databases, etc. can cope with a change of date to a new century the effect of those date changes affects the organisation.

Without full management, you cannot be sure that sufficient resources will be made available to address the problems.

What are the benefits of the work?

This will clearly be needed to get the full support of management to provide the resources necessary.

The benefits will include reference to:

- Achievement of business goals
- Survival of the business

What are the risks involved?

Need to identify the risks associated with the work. This includes:

- Time constraints
- Complexity of the changes required
- Availability of resources
- Need for specific skills

What elements will need to be addressed?

These will include:

- Hardware
- Systems Software
- Application Software
- Documentation
- Training
- Maintenance
- Operations
- Administration
- Acceptance criteria for all deliverables

Who will need to be involved?

This will include:

- User Management
- IS Managers
- System analysts
- System designers
- System/Application Programmers
- Operations personnel
- End Users
- Auditors
- Quality Assurance
- Hardware, software and application vendors
- IT outsourcers
- Consultants

Consultants

When using consultants, expect to spend at least 25% of the time to explain how the applications work. Depending on the complexity of the applications, some project managers may spend 100% on this for several weeks.

If off-shore resources (or the like) are used, system integration testing with real production data has to have the highest priority, otherwise, it's a roll of the dice. Management should plan to have in-house people do this for however long it takes.

Inventories

It is obvious that most of the planning process cannot be carried out without a knowledge of the extent of the problem. The first step that must be carried out during the planning process is to create an inventory of all the IT elements.

This will allow you to analyse the IT elements to identify where the date-related processing occurs and to track and control changes to these elements.

Inventories need to be set up for each of the following types of IT element:

- Hardware
- Systems Software
- In-house developed Application Software
- Proprietary Software purchased from vendors
- Other "non-obvious" areas where automated date processing may be involved (such as PABXs)

Priorities

For each of the IT elements which carry out date related processing, the criticality and priority of each element needs to be determined. This is in terms of how critical the functions of each element are to the business.

Many factors will contribute to determining criticality. These will include pressure from customers or suppliers, legal, financial, or political issues. The major factor should be the impact on the business.

The following categories could be used for considering the priority for work:

- Is it critical to the operation of the whole business?
- Is it critical to the uninterrupted operation of the business?
- Is it required to support the business?
- Is it desirable, but not absolutely required to support the business?

The impact on the operation of the business processes also needs to be taken into account. Here, you should be considering:

- Will failure cause the process to terminate?
- Will failure produce an incorrect result (e.g. incorrect interest calculation)?
- Will it result in misleading information (such as a date printed incorrectly on an invoice or a statement)?
- Will it merely be a minor irritation with no real affect on the business (although customer irritation can result indirectly in loss of revenue)

There are various software tools to help perform the "impact analysis." Any large company not using some of the available software tools will probably need more programmer time on the project.

Even if you are using software tools to carry out impact analyses, remember that they are not infallible. There will be many instances where dates are referred to in program code where data naming standards have not been followed. Many programmers would refer to data by their own unique names rather than following laid down rules. You will still need to do a considerable amount of manual checking of code.

Each organisation needs to do an inventory of their applications and the production programs within each application. The JCL can be tied into the mainframe load modules. Is there production source code related to each production load module (& vice versa)? Are any modules no longer used in production (the number may prove surprising)? You probably do not want to use programming resources to convert unused code to the year 2000.

It is recommended that you also determine which applications will be replaced in one, two or three years. It may be unnecessary to modify these programs, although this depends on the ability of the IS Dept to deliver replacements on schedule. Review of the interfaces between applications is very important.

Financial systems should be the highest priority - they have the most effect on publishing the balance sheet. They also have the earliest critical time window — completion in 1998, not 1999, to ensure a fiscal cycle gets completed on revised code.

The "impact analysis" (or "risk assessment") phase often seems to involve only limited resources spread over 3 to 12 months. You may want to consider assigning more resources to this early phase and speed-up your schedule. You may want to conduct a pilot "impact analysis" on a small mainframe application using software tools. Next, have each lead system analyst for the other major mainframe systems perform the same process with input from the person who conducted the pilot. You may want to use a consultant (or someone from a company that has done this) to review your "impact analysis" for each system. I have noticed that some companies seem to let the consultant's conduct most of the "impact analysis" and it seems to be the same process performed 5 to 12 times sequentially instead of concurrently. If the tasks are performed concurrently, a company may be able to finish their project earlier. While carrying out an impact analysis is seen to be crucial to ensuring best allocation of resources, there is a danger that the impact analysis will become the priority and very little else will be done. There is benefit in carrying out a pilot as part of the analysis and then feeding back the results of this pilot into the overall plan.

Since the cost for the "year 2000" projects is said to be going up 30% or more per year, you may be able to speed-up the schedule and save money. Even if the work done concurrently takes more person days of programmer time, you may save because the implementation phase, which is later, is where most of the programmer time will be needed. In essence, you may be able to save money by taking steps to speed-up the schedule. (However, the learning curve, related to using the impact analysis software tools may be so great that it may be more efficient to have only 1 to 3 people perform all impact analysis work.)

Timing/Delivery Dates

The critical dates for each different organisation will be different. For each application affected, an analysis will need to be done to determine when the effects will first be felt. This is the absolutely final date by which the conversion must be done.

Corrections need to be done in time to run at least one monthly, one quarterly and one year end before you need the system to be compliant. As such, a system that needs to be compliant by 31st December 1998 should be done no later than 30th September 1998. Obviously, people will fall short, and will have to try to run all three at the same time. But, if you have time, this is a better way. In that way, you have a bit more time to react and look ahead.

Ownership and Identification of Users

In order to help co-ordinate the work, you will need to identify both the owners and the users of affected data. These can be sub-divided into the following groups:

- Data which is created and processed exclusively by a single business area. Here there will be a single owner and user.
- Data which is created by one area and used by themselves and by others. Here there will be a single owner and primary user with potentially multiple secondary users.
- Data object is defined and created by the organisation and which is distributed to other organisations. Here, the users could potentially be outside the control of your organisation.

- Data which is created outside your organisation and which is subsequently imported. In this case, the owner of the data may well be outside the control of your organisation.

Standards and Guidelines

To avoid confusion and further problems, which can be created by having several different technical solutions to the issue, it is important that standards and guidelines are established early in the project. These would include:

- Whether the preferred solution was to be through the use of program logic or through the redefinition of stored dates (increasing stored year to 4 digits for example).
- Ensuring that Year 2000 was taken into account in the specification of new hardware and software which was acquired for unrelated business purposes.

Finding the exposures

Perhaps the most difficult aspect of the work will be to identify all the occurrences of date related processing within all the programs used by your organisation. A structured approach to this identification is called for.

A checklist for identification of date related processing is as follows:

- Create an inventory of every program entity used by your organisation.
- For each program identified, review the following documentation for references to dates tracing these references back to the application source code to locate references in that code as well.

- Feasibility studies
- Systems specifications
- Systems design documentation
- Program specifications
- Program code
- User instructions and procedures
- Data entry forms, screen display formats, report formats
- Definitions of data fields, records, structures, files, and databases
- Data dictionaries

Review program source code for date references

This can be automated by searching for specific character strings which would normally be used to denote date processing. Many consultants and vendors have produced automated tools which can assist in this identification. However, they will never find every occurrence of a date, mainly because programmers have never adhered to programming standards, even if these standards have been available.

Use of a test system can allow you to identify many exposures. It is important, however, to ensure that this test system is isolated from your production systems so that any corruption which may occur does not contaminate your systems. There are two basic methods that can be used:

- Use it to process data with future dates set to ensure that these dates can be coped with using existing systems.
- Set the system date to a future date to ensure that the systems can cope with the transition between centuries. It is very important that this type of testing is not carried out on production systems as unpredictable results can occur. For example, there are reports of companies who have done this and have had vital backup files automatically deleted as their expiry dates have been passed (how many of your installations use 99/99/99 as an expiry date for files which you don't want to be deleted? What will happen to these when you move into the next century?)

Once individual exposures have been identified, it would be prudent to trace the processing logic between programs to ensure that all interactions and related processing had been identified. It must be appreciated that where the degree of date sharing between programs is high, then the more critical will be the task of correcting the problems.

When looking at source code - program library combinations, don't forget about subroutines. Subroutines can remain hidden and their source code is often the most difficult to track down.

It has been suggested that the Year 2000 investigations are a good time to carry out reviews of application code to eliminate unused program modules and to identify and eliminate unused code within programs. However, this all adds to the cost of the project.

Does all the object code have corresponding source code and does the source match the object? How will we show this to be the case?

Correcting incorrect date formats

There are a number of techniques which can be used to correct improper dates. There are advantages and disadvantages to each. Each organisation must choose which is most appropriate for its own needs.

An up front decision should be made on whether to add logic to manage a sliding century window or to expand fields. The latter poses much additional cost in devising and managing I/O translation bridges for "old" data, which is probably 90+% of all data available. Of course, some applications may require adopting the costlier approach.

This approach can be thought of as the only definitive final solution to date problems. It will ensure that the problem will not recur, provided the standards for dates are followed for all future developments. It requires changes to both the data and the programs.

There are problems however.

Migration of data and programs will be extremely complex. Because of the complexity and interrelationship of most applications, a change to one application will inevitably affect other applications which have yet to be converted. Bridging mechanisms must also be developed to convert dates when they are transferred between incompatible applications.

There will also be increased workload as data structures have to be altered.

In addition, some programming languages may not allow for dates in this format.

Windowing Techniques

Fixed Date Window

This uses a fixed 100 year range where the two digit year is compared against a range of year values within the window.

For example, the window could be defined as lying between 1970 and 2069. In this case, year 10 would equate to 2010, year 25 to 2025, year 75 to 1975 and so on.

This will enable current programs to deal with existing 2 digit year formats with only the addition of date conversion modules and processing to link it to relevant programs.

However, this fixed range will need to be reviewed every year to ensure that the range is still appropriate. In addition, as mentioned above, there will be circumstances where the range will no longer be appropriate.

One other problem which can occur is that historical data may be corrupted when it falls outside the lower limit of the window.

Sliding Date Window

Here, the same concept of a 100 year range of dates is employed. In this case, the range advances automatically every year to ensure that the range is a constant number of years before and after the current date.

This has similar drawbacks to the fixed date window, although processing is automatically adjusted to change the date range.

Digit Encoded Dates

Using the two digits which are currently used for representation of the year, it is possible to devise an encoding scheme which will allow the century plus the year to be represented in two bytes.

This is another approach to be cautious about. Even though there would be no need to expand storage definitions, a considerable amount of effort will be needed to ensure that all current programs can handle the new compressed date format. In addition, much discipline will be needed to ensure that this format is perpetuated in future developments.

Remember also that historical data will also need to be converted, especially where it is needed to provide management information comparisons.

Standards

It is considered vital to develop a standard for date handling that is rigidly enforced for both legacy and newly developed systems. It is no use expending effort now to clean up the problem if it can be reintroduced by existing system maintenance and future developments.

Backwards compatibility

You will need to ensure that any new processing logic which is implemented is capable of handling historical data where analysis of this data is required in the future.

Other Changes

When the source code to be made year 2000 compliant is copied to a separate library or sent to a consultant via tape or other method, should routine changes to the production code be made? Routine changes can be made, but it appears best to minimise the changes. The more changes made to production code, while the programmers are making the other code Year 2000 compliant, the more difficult it will be to merge those changes with the code which has been made Year 2000 compliant. A very strong attempt should be made to limit the changes to those necessary to fix a system which has "bombed."

Efforts should also be made to minimise organisational changes while the Year 2000 code changes are being made. The users and your company will maximise programmer resources by minimising these interim changes. (Does everyone really believe that Sr. mgt. will never permit such a freeze on system changes?)

If parallel development/rescue maintenance is to be allowed, the "code merger" should be installed and tested BEFORE its use is required, and standards for use implemented before that. It's too late if you're trying to merge code for a financial system, for example, and the fiscal year end is coming up.

Testing

As with all systems development, one of the most important keys to success is thorough testing of all aspects of the work. Program, system and acceptance testing all need to be performed to identify errors and, more importantly, to ensure that user pre-defined processing results are achieved. These tests should ensure that the amended systems operate in both normal pre-2000 conditions and in post-2000 conditions.

Testing is much more complex than most people realise.

If you do not have a separate test environment with test data packs that mirror the production environment, then there will be grave doubts about the ability of the amended systems to cope with production. If this is the case, you would be well advised to set up a proper test facility as a matter of urgency.

The test plans to be used, during the implementation phase, can be 80% or more completed by the time the plan (for implementation) is completed. What will be needed for a test plan? If you were a computer consultant, besides the source code, what would you need to see in order to set up the process? An experienced project leader should be able to tell you the types of test plan documentation, which would be needed. The lead systems analysts should be able to fill in more details, related to their system. The lead systems analyst should be able to co-ordinate the creation of test data, along with information about the way the system works. An organisation does not need to wait until the "impact analysis" and "plans" are created to begin to prepare the test plans that will be needed during "implementation." They will need to update the test plan prior to segregating the code to be made "year 2000" compliant.

A good project manager should be able to lay out what will be necessary for "acceptance testing" after the code changes are made. The lead systems analyst for each system to be changed should be able to flesh out the remaining details for the "acceptance test" for their system.

Suggestions for types of test plan documentation required include:

- Test scripts
- Data
- Expected results and expected exceptions
- Regression test plan

There are products that you can use to set the date forward and backward. This is a great way to test a vendor system quickly.

Pre-2000 Testing

This should be no problem if you have a stable, separate test environment. Carry out testing in the same way as you would for any new application development.

Post-2000 Testing

By necessity, this requires that you run your tests with a systems date after the turn of the century.

But, you must be careful before resetting the system timer. Some system software may be date sensitive. Some software products will not operate after the licensed expiry date of the current license. Also,

you may find that resetting the system date will result in critical data files being deleted (past their retention dates) and tapes will be scratched.

This really serves to emphasise the recommendations of the past that there should be separate testing environments within which proper testing can take place without impacting production processes. The introduction of such environments has regularly been rejected on cost grounds. Testing for Year 2000 compliance is going to introduce additional cost. However, try to sell these enhanced facilities as an investment for the future, rather than as a knee jerk reaction to past indiscretions.

There are some software products which will allow you to capture the systems date which is returned following a call to the system and to change it to a user determined date. These are worth investigating. However, remember that you must also investigate the potential undesirable effects of date changing as mentioned above.

System Software

There are suggestions that some software vendors will not be able to supply changes to their products and will merely file for bankruptcy when their products fail and the inevitable lawsuits start. Also that some software vendors do not now exist (although their products are still in regular use). It is vital that this aspect of Year 2000 is investigated soon in order that alternative products can be identified should any of the products in use follow this scenario.

Software vendors need to address those products which provide infrastructure support - such as sort utilities, database managers, backup-restore programs (many of which operate based on time of day comparisons), data manipulation tools, system performance monitoring software, unattended operations managers, security software, system maintenance software, etc. Those things that are not quite O/S and not quite applications - but are key tools.

Hardware

The Year 2000 problem is not only related to software, but in fact may well be a hardware problem also. The underlying hardware may not be able to support the software as hardware clocks wrap to some unusual value. One needs to have an understanding of the underlying technology capabilities and limitations also. Older PC's with old BIOS installed may not be able to continue functioning in the future because of this problem.

Vendor Supplied Software and other issues

All of the above supposes that you only operate in-house written bespoke software.

This is not the case.

You will also have system software, purchased application packages (potentially tailored for your own business) and applications which have been written for you by third parties (do you have the source code?).

Therefore, in addition to examining your own in-house written code you must also contact suppliers and gain assurances that the software which they have supplied is Year 2000 compliant and, if not, it can be corrected within a time scale that is specified by your business.

Contingency planning is also essential. Consider the utility software that you have been using for many years where the original provider is no longer in business. What do you intend to do about this? Potentially, you must search for alternative products.

Staffing the project

Who do you need to provide resources for the Year 2000 project?

If you are reliant on legacy software which, most likely, does not provide for the change of century and which (also most likely) is insufficiently documented, who can you call on to provide knowledge and expertise?

Why not try the people who created the problem in the first place?

Most companies will still employ some of the original programmers who, through their desire to create efficient programs, introduced the problem in the first place. While they have probably now moved on to fill senior management positions, they are probably the best placed to interpret the programming logic of the programs which will cause the most problems.

Use them!

Automated Tools

Year 2000 tools are being produced faster than they can be reviewed.

A wide range of tools is available from software vendors and consultants covering impact analysis, program analysis, code analysis, automated testing and so on.

Unfortunately, none can guarantee total success in identifying and resolving the date problems. There are no "magic bullets" or definitive solutions.

The best advice is to use automated tools as much as possible, but not rely on them. The use of the human resource is considered to be the only effective solution.

Benchmarking

If you have not really started working on a "year 2000" project, you should promptly try to benchmark with companies (or other comparable entities) that are 6 months to a year into a "year 2000" project. Any company which has not made that much progress is likely to provide you with misleading information. I believe that nearly all large companies which have not yet begun a year 2000 project have not benchmarked with the proper companies to determine what steps they should be taking.

Each company which has not started their "year 2000" project should list the major applications which they believe are compliant.

Will the vendor confirm it is compliant? If the vendor will not quickly verify in writing that it is compliant, you should assume that it is not compliant.

If you have any customised code related to the application, it must be compliant so you need to test it for about a month before you ASSUME that it is compliant. You can also check with others who use the product to determine whether they have conducted extensive year 2000 testing to confirm it is compliant. I am amazed at how many companies continue to ASSUME that their vendor applications and the related customised code is compliant but they have not performed any testing. The "proof should be in the pudding".

The failure to both confirm with others and conduct very extensive tests is a prescription for a disaster. (Almost a planned disaster)

What should you be able to determine by performing "year 2000" benchmarking with those who are 6 months to a year into the year 2000 projects?

You need to start on these projects NOW instead of later. (The projects should have been under way for nearly a year.)

The resources needed for a year 2000 project are HUGE. (The Information Technology Department and Internal Audit Department may not have time to handle any other strategic initiatives. You will need more DASD and the longer you wait the more likely it is that you will need a mainframe upgrade.)

The scope or size of these projects is company-wide.

The projects will take extensive time for your Information Technology Department, users, and even auditors.

Never ASSUME that an application is year 2000 compliant until the following has been done:

- The software vendor has confirmed in writing,
- The customised code has been tested for about a month to verify that it is compliant,
- There are other users of the vendor software who have performed the same steps and come to the same conclusion, and
- The auditor reviews it to see how it works here and now on the system being used.

Please be sure that you benchmark with companies that are 6 months to a year into these projects. Anything less is may be like seeking advice from a "tree stump".

If you fail to benchmark with the correct companies, you are probably taking a significant risk that you will come to the wrong conclusion. We all know what happens when we ASSUME. Please cover your risks.

Anyone into this project for six months will most likely not have done much testing nor any file conversions. Since those are fairly time consuming tasks, you will only have 50% of the information.

What if it fails?

If, on the 1st of January 2000, your automated application processing fails and the continuance of your business is in jeopardy, what do you do?

Have you considered insurance?

Have you considered the liability of your Directors in the event that the business fails through predictable means?

While the world will not end on 1st January 2000, there will be some grief. Not all programs will work. The prudent organisation will make sure that it is the insignificant programs which will fail. Those who do not start the conversion investigation work now and supply enough resources will have problems which could seriously jeopardise their ability to continue trading.

If businesses fail, it is not just a few company directors or senior IT managers whose careers are shortened. There will be an serious effect across the whole value chain.

Legal Liability

Year 2000 can and probably will result in legal liability. Vendors will fail to supply hardware and software which can cope with the date change and may be open to litigation. However, what consolation is it to sue someone for failure to supply a working product when your business is going to fail whether your legal action is successful or not?

What about the legal issues which attach to company directors and officers?

Do your directors and officers understand their legal liability risk in this area? Do your legal advisers understand the problem and its ramifications?

When corporate officers and directors act in a "reasonably prudent business manner", it is nearly impossible for shareholders to recover from them individually. Have your corporate directors and officers acted in a "reasonably prudent business manner" if they fail to take appropriate action on the year 2000 computer problem (since it is a foreseeable event)?

They would probably not be viewed as having acted prudently if they failed to take timely action and allocate enough resources. Could they be held individually liable in a shareholder class action lawsuit? Probably so!

If the Director & Officer Liability insurance policies are changed to limit or exclude coverage for the year 2000 problems and its ramifications, then officers and directors could be jointly liable, with little or no insurance coverage. This fact should serve to concentrate some minds.

Audit questionnaire

The following questionnaire is offered as a sample of the questions that Internal Auditors should be asking within their own organisations to ensure that the conversion work is properly planned and will be carried out correctly within the desired time frame.

Management Awareness

Q.1 (a) How have senior management / board been made aware of the Year 2000 issues? (b) Has Management set an organisation goal to have the business ready for Year 2000 before any disruption caused by 2-digit-year data occurs? (c) How has Management communicated this goal?

Q.2 What actions relating to Year 2000 have been approved by management?

Q.3 What priorities have been established?

Q.4 What timetable has been set?

Q.5 (a) Has a Year 2000 Project been set up? (b) Are user management actively involved in the project's progress?

Q.6 What Year 2000 standards have been established for on-going enhancements and future developments?

Business Horizon

Q.1 (a) When will the impact of Year 2000 first bite? (b) Have 'critical event horizons' been established for key business activities?

Q.2 Have 'similar horizons' been encountered previously, either related to Year 2000 or other date issues? If so, will the solutions implemented remain valid for Year 2000?

Resource Requirements

Q.1 What estimates have been made of the resources / budgets required to address the Year 2000 problem?

Q.2 Has an assessment been made of the staff and IT system

resources needed to test the changes made for Year 2000?

Q.3 What impact will 1 and 2 have on on-going maintenance and future developments?

Q.4 What assessment has been made of any additional hardware capacity requirements?

IT Planning

Q.1 What steps have been taken to assess the impact of Year 2000 on applications ?

e.g., have inventories been made of :

- applications / programs performing date calculations
- packaged software (supported and unsupported)
- end-user developed applications
- programs where source code is not available
- program languages (supported and unsupported)
- databases where dates form part of a key field
- interfaces to / from third parties

Q.2 What steps have been taken to assess the impact of Year 2000 on operating systems and system software?

e.g., have inventories been made of :

- operating systems (supported and unsupported)
- security systems
- database systems
- compilers (may or may not support Year 2000)
- firmware ditto
- other system software

Q.3 Has an inventory been made of all the types of platforms used, including PCs?

Q 4 What strategies are being considered for resolving Year 2000 problems?

- change all dates to four digit years
- develop program solutions and keep two digit years
- big-bang or piecemeal developments
- bridge programs
- rely on package vendors to supply solutions

Q.5 What conversion work or piloting of conversions has been carried out?

Other

Q.1 What steps have been taken to assess the impact on tape / archive management systems where dates such as 9/9/99 or 31/12/99 could have been used to indicate the data should not be deleted?

Q.2 What impact will Year 2000 have on PABX and other communication systems that may be date dependent?

Q.3 What impact will Year 2000 have on electronic security and alarm systems that are date dependent ?

REFERENCES RELATED TO THE YEAR 2000" PROBLEM

Print Media References

1. — January 1, 1996 issue of DATAMATION has 5 articles and an editorial. This is an excellent resource. The Internet reference is http://www.datamation.com Also, page 102 of the May 15 issue has a good one page article by Peter De Jager.

2. — CIO magazine dated December 15, 1995 January 1, 1996 is a special edition. The article starts on page 82 and it is a good non-technical article. This article appears to be one which you may want to share with management.

3. — March 1996 issue of PC Novice has an article on pages 54 & 55.

4. — Software Magazine January 1996 issue has an article on pages 27 & 28.

5. — Computer World has had several articles over the last several years.

The September 6, 1993 issue has an article called "DOOMSDAY 2000."

The February 12, 1996 issue has an article called "1418 days and counting" and the subtitle says "CA offers year 2000 date-change products." The March 25, 1996 issue has an article on page 83 called "Face up to it" and page 86 has numerous references including conferences, user groups, and other resources. The April 22, 1996 issue has an article on pages 1 and 117.

6. — Enterprise Systems December 1995 has a small segment on page 6.

7. — Millennium Journal 1-(800)708-0675

8. — Financial Times 7 February 1996 issue has a year 2000 section.

9. — The February 5, 1996 issue of INFORMATION WEEK has 2 good articles.

The first begins on page 30 and the second begins on page 44. The April 15, 1996 issue has an article beginning on page 66, which discusses "How to assess your year 2000 conversion effort."

10. — The February 1996 issue of APPLICATION DEVELOPMENT TRENDS has an excellent 2 page article "10 pitfalls to avoid in the year 2000 initiatives"; however, even their good corporate-wide scope does not address the outside service providers, vendors, and customers with whom the "year 2000" team needs to communicate early in their process.

This magazine is a sister publication to the AMERICAN PROGRAMMER referenced below. The July 1996 issue has a good article starting on page 56.

11. — On Friday March 8, 1996 the newspaper USA TODAY included an article in the Money section. The article heading was "Year 2000 poses computer software headache."

12. — The February 1996 issue of the AMERICAN PROGRAMMER has 6 articles on "The Year 2000 Problem." Their telephone numbers are (617)648-8702 and (800)964-8702. The "Systemic Triage" article by Peter de Jager is one of my favourites and it was included in the handout materials provided by Computer Associates at their one day seminars on the "year 2000."

13. — The May 1996 issue of EDPACS (The EDP Audit, Control, and Security Newsletter) has a 13 page article on "A Strategy For Handling The Year-2000 Problem."

14. — June 1996 issue of INTERNAL AUDITOR includes an article starting on page 12 and resources are shown on page 16.

15. — June 24, 1996 issue of NEWSWEEK has an article on page 92.

16. — July 5, 1996 issue of the Wall Street Journal has an article on page B2. July 25 issue had an article "The Year 2000 and the CEOs' Big Secret" on page C1. July 26 issue had an article on page B1 "Businesses Make A Date to Battle Year 2000 Problem."

17. — July 1996 issue of CFO magazine, which is read by nearly all Chief Financial Officers, has on page 16 "Countdown to Year 2000."

18. — July 29, 1996 Forbes magazine has an article on page 35 by Caspar Weinberger.

— Internet References —

1. — http://www.year2000.com This site has numerous good references including the "Systemic Triage" article and "2001: A Legal Odyssey."

2. — http://www.software.ibm.com/year2000

This is IBM's Web site and it has some very good information. Another IBM Web site is http://www.s390.ibm.com/stories/tran2000.html

3. — http://www.cnn.com — select technology and the January 7, 1996 report by Jed Duvall titled "The year 2000 does not compute" may still be there

4. — Year 2000 NEWS is free if you send an e-mail with SUBSCRIBE in the subject field to news2000-request@andrew.cais.com. To stop your subscription send an e-mail with UNSUBSCRIBE in the subject field. You may want to request prior issues from rarnold@cais.com

5. — There is a mail list to discuss the problem. One can join by sending a message to listmanager@hookup.net with the message SUBSCRIBE YEAR2000 in the body of the message, not the subject.

6. — http://www.isaca-chicago.org — The Web site for the Chicago Chapter of the Information Systems Audit and Control Association (ISACA) may be useful.

7. — http://www.cai.com/products/ca2000/disc2000.htm is a Web site run by Computer Associates.

— Other References —

1. — Computer Associates conducted 20 one day free seminars around the U.S. during February 1996. Call 1-800-225-5224 for additional information.

2. — The Software Productivity Group has sponsored several 2 day conferences and expos. Call (508)366-3344 x 244 for additional information. Their November 1995 conference in Orlando had over 600 attendees and I understand it was a very good conference. They are likely to have other training sessions on the "year 2000" during 1996.

3. — Ask the audit partners & consultants from the Big Six about the problem.

4. — Ask your IBM representative about the problem.

5. — Ask your Computer Associates representative about the problem.

6. — Ask the "year 2000" project team members of any large organization which is working on the problem. You may want to try any large bank, large insurance company, or large utility company.

7. — On Thursday March 7, 1996 National Public Radio (NPR) carried a news story on the "year 2000" problem.

8. — On Monday evening April 15, 1996 the Jim Lehrer News Hour on educational television had a segment on the "year 2000."

9. — The Gartner Group is conducting many one day seminars. They have been among the leaders on this topic — 1-(800)645-6395 and 1-813-733-3666.

10. — Audit Serve is conducting several 2 day seminars for auditors. Their telephone number is (203)972-3567. http://www.auditserve.com

11. — Ask your application programming supervisors and lead systems analysts about the "year 2000" problems which your organization is facing. Ask each one whether they have read any articles on the topic. I believe that these individuals usually know the magnitude of the problem but they may be reluctant to comment for several reasons.

12. — Ask the largest MIS Dept.s in your region about the problem.

Acknowledgements

This briefing note has been compiled from a variety of sources.

For permission to use their material, specific thanks to:

Tom Crouch, EDP Audit Coordinator, Kentucky Utilities Company

Clive O'Connor, Group Internal Audit, Bank of Ireland.

For positive comments following review - Ed Barth, Fidelity Investments

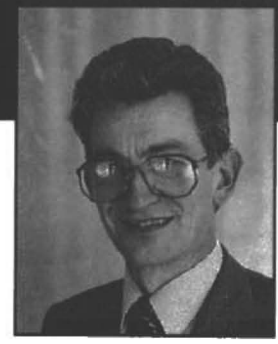
---

Alan Oliphant is the editor of the Opinion column in this Journal. All opinions expressed are his alone (and a combination of others') and not necessarily those of his employer. Feedback on this article should be sent to: alan.oliphant@msn.com

Submission Deadlines

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

BCS MATTERS



Colin Thompson

The BCS Deputy President

Let me start by correcting one serious omission from my last piece for this journal which gave a run down of the new Senior Officers of the Society. Looking back over that article recently I noticed that I had left out one very important name - Sir Brian Jenkins GBE, MA, FCA who became the Deputy President at the 1996 AGM.

Sir Brian is Chairman of the Woolwich Building Society and a Committee Member of the Automobile Association. Until his retirement at the end of April 1995 he was a senior partner in Coopers & Lybrand and was, between 1986 and 1991, Head of the Audit Practice. He has been Lord Mayor of London (1991-92) and President of the Institute of Chartered Accountants in England and Wales (1985-86). If the coming year follows the normal pattern, Sir Brian will succeed Ron Mcquaker as BCS president at The AGM in October 1997.

1997 Annual Dinner and the 40th Anniversary

The annual dinner is traditionally the first official engagement for the new President each year and this year's event, scheduled for 17th October will have a special significance as it marks the start of the Society's 40th anniversary year. In recognition of that the 1997 dinner will be supported officially by the worshipful company of Information Technologists and will be held in the Guildhall.

A range of other events are being planned during the year to mark the anniversary and I hope to bring you further news of the programme in the next edition of the CASG Journal.

The BCS IT Awards

The British Computer Society IT Awards are amongst the most prestigious in the IT industry and this years competition produced another very impressive crop of innovative IT projects. The "excellence" which the Awards recognise can take many forms. The judges normally expect to see some degree of originality and innovation. Other relevant factors may include speed of implementation, quality of project control, significant cost savings, width of applicability, commercial success, popularity with users, integration of discrete technologies, social or educational benefits.

During the course of the 1996 competition the judging panel saw around 90 projects and eventually selected the following 11 medallists:-

Clicker Plus - a communication aid for the disabled by Crick Computing, Northampton

MAVIS - an instrument to measure wounds by Dept of Computer Studies, University of Glamorgan

ScotWeave - a woven fabric design system by SCOT Innovation and Development Ltd, Galashiels

QUESTAR - Neural Network Analysis of Sleep Disorders jointly developed and marketed by Dept of Engineering Science, Oxford University and Oxford Instruments

IP+ - The Intelligent Prosthesis Plus a device for amputees which automatically adjusts the swing of a limb by Chas A Blandford & Son, Basingstoke

Microcosm Plus - an IT solution which allows access to existing archives and aids better information applications in education by Multicosm Ltd, Southampton

Peritas Online - an on-line interactive Internet service offering a range of technical and end-user training courses by Peritas Ltd, Berkshire

Pindar Catalogue Management System - a product which enables users to efficiently produce promotional materials from text and graphics stored in a single comprehensive database by Pindar plc, York

INCA - Inter-Network Call Accounting - a tracking system to bill other operators for their BT usage by British Telecom, London

INDEX+ - a comprehensive infrastructure for the creation, management and development of text and multimedia information services e.g. National Gallery, by Systems Simulation Ltd, London

Sibelius 7 - as an expert system for music, it incorporates many hundreds of rules of music notation and engraving to produce publication quality output, by Sibelius Software, Cambridge

All 11 projects were on display at the Institution of Civil Engineers on 10th February, when the 3 overall winners of the 1996 awards - Microcosm plus, INCA and Sibelius 7 made presentations to an audience of around 220 people. The event was hosted by the Duke of Kent and Kate Bellingham, one time presenter on Tomorrow's World, was the guest presenter.

Further information about the above projects, and about the 1997 competition, is available from Anna Duckworth at BCS HQ.

A Driving Licence for your Computer?

The BCS has signed an Agreement for the European Computer Driving Licence (ECDL), which provides a Europe-wide qualification of competence in the use of Personal Computers (PCs).

The Licence will be delivered in the UK through accredited providers of PC skills testing, who have demonstrated compliance with the ECDL syllabus and testing requirements. This will operate initially in pilot mode with the National Computing Centre (NCC) as the provider. Following the pilot period we expect to start accreditation of a range of user PC skills providers, including NVQ Awarding Bodies. Discussions are currently in progress with the Information Technology Industry Training Organisation (ITITO) to establish syllabus compliance, which will then be made available to all the NVQ Awarding Bodies."

Similar licence arrangements are already in place in some Nordic countries, and pilots are underway in France and Ireland. The concept of a computer driving licence was pioneered in Finland, and adopted in 1996 by CEPIS, the Council of European Professional Informatics Societies, of which BCS is a member. The European Commission is committed to its development, and the European Computer Driving Licence Foundation, which operates the ECDL arrangements on behalf of CEPIS, is already working with the Commission on the full access provision to

the licence throughout the European Union.

For further information - Anna Duckworth again.

The Millennium Problem

The year 2000 problem continues to be the hot issue of the day and it is clear that this will continue as we approach the millennium. The BCS publication The Year 2000 A Practical Guide for Professionals & Business Managers has proved extremely popular and we have been forced to reprint to meet demand. The book is available at £7.50 to BCS members and £10.00 to non members. Orders for the book should be forwarded to the Marketing Department at BCS HQ (telephone 01793 417424 or e-mail marketing@bcs.org.uk).

BCS Registers

Work is continuing on the proposed new BCS registers - the Security Register and the Consultancy Register - which I mentioned in my article in December. The Security Register will be a fully validated public register of security specialists and we expect to be taking applications for registrations by about the middle of the year. Further information will be provided in future editions of this column, but I am maintaining a mailing list for those with a particular interest. Drop me a line, or an e-mail message if you would like an information pack when it becomes available.

The Consultancy Register Task Group is working towards a report to be submitted to the AGM in October. The group plan to publish a "green paper" in April, which will set out proposals and options for comment. A summary will be carried in the April Computer Bulletin and the full text will be available on the Web. Anyone requiring a paper copy should let me know.

Secure Computing

Still on the security theme, we now have an arrangement with the publishers of the periodical Secure Computing for free delivery to BCS members and members of relevant specialist groups. Let me know if you would like your name added to the list.

And Finally.....

A reminder that the Society welcomes applications for membership - for both professional grades and for the new Companion grade - from CASG members. If you are not sure whether you are eligible for membership simply complete the form attached to the brochure enclosed with this edition of the Journal and we will provide specific advice.

Colin Thompson is the Marketing Director for the Society and can be contacted at BCS HQ, 1 Sanford Street Swindon SN1 1HJ, telephone 01793 417410 e-mail cthompson@bcs.org.uk

Letter to the Editor

As an overseas based member, I would like to congratulate the Committee both on the quality of the Journal and both the scope and topicality of the Technical Briefings.

For the benefit of those of us who are unable to attend the sessions in person, I'd like to request that, where possible, speakers' papers for these sessions be published in the Journal.

I am sure that this would be of great benefit, not only to those of us who are located as far away from London as it's possible to be, but to the many UK based members who are unable to attend the sessions because of work commitments.

By the way, I would like to commiserate with former colleagues on the severity of the weather in the UK at the moment (30th December). If it is of any consolation, it was a bit of a relief to get out of the sun and into the airconditioning this morning.

Bob Ashton
Brisbane
Australia

It is always nice to hear from our overseas members. We do endeavour to include papers from our technical briefings, but in many instances they are not suitable for publication due to their format. -Ed

REPORT FROM THE CASH BOX

Bill Barton - Treasurer

We are now well into the second half of our financial year, and therefore it is timely to update you on the state of the group's finances.

Our core income comes from membership subscriptions. Subscriptions received to-date are approximately £5,700, slightly down on the prior year. We have also earned £800 from bank interest.

The technical briefing day in October, held in conjunction with the IT Faculty of the Institute of Chartered Accountants in England and Wales, resulted in a profit of £250. We are finalising the costs for the second technical briefing day in January, which had just under 100 attendees. The current estimate is there is a profit of approximately £1,500.

Our main area of expenditure other than the technical briefing days is on the journal. Costs, net of advertising, for the first three of the four journals issued this year are £3,500.

Our objective for the year is to break even at least. Whether this will be achieved will depend on the final technical briefing day on 15 April 1997. It will cover systems development audit and I urge everyone to attend.

We still have approximately £25,000 in our bank accounts and continue to be open to suggestions as to how this money can be usefully applied. *(I keep suggesting research topics based in the South Seas, but the Chairman keeps vetoing them - Ed)*

William List
Chairman of BCS Security Committee

Do you want to know more about the latest developments in computer security and standards that affect your work as a computer auditor? Do you want to help formulate BCS comments on draft standards, or government security guidelines, before they are issued? If so, read this article about the BCS Security Committee. There is a degree of overlap in the work of that committee and our own group and it is not too surprising to find that the Security Committee's chairman is a past chairman of the CASG - Ed.

The BCS Security Committee

William List - Chairman

Within the Society there are a number of Committees and Task forces reporting to the Professional and Public Affairs Board (PPAB) whose task it is to advise Council, through the Board, on matters relating to the policy of the Society in all professional matters such as issues of importance to the Society, registers of experts in various fields and to prepare the formal Society responses to the myriad requests for comment from EC, OECD and Government.

The Security committee is the Society's standing Committee which covers the Computer Security area. Its terms of reference and constitution are set out below:

Terms of reference

The Committee is responsible to the PPAB for:

- Monitoring the field of computer security, with the objective of formulating policies which the Society can endorse.
- Keeping under review factors such as technical developments and professional attitudes and behaviour which are likely to influence computer security in all its aspects including, physical security, software security, security within communications systems and security involving personnel.
- Considering ways of providing systems security against both deliberate and accidental threats, and also providing guidance on monitoring the effectiveness of such measures, and minimising the disruptive effects of events that occur.
- Liaising with other Society committees and Boards as appropriate, in particular the Data Protection Committee. Liaising with external bodies as appropriate.
- Advising on policies, positions and activities the Society should adopt.

Constitution

Members of the Committee are normally Fellows, Companions or Members (of any grade) of the Society.

The Chairman is appointed by Council on the recommendation of the PPAB.

Vice-Chairman are appointed by PPAB on the recommendation of the Committee.

Members are appointed by PPAB on the recommendation of the Committee.

The Committee is fully aware that it cannot, within its own resources, represent all views in the Society. It has therefore set up a series of teams each led by a committee member to keep up to date in specific areas, identify issues which the Society should be aware of and to do the main work of preparing comments on documents.

As a flavour of the work of the Committee the following tasks have been undertaken during the last year:

- Comments have been drafted on: The Common Criteria, BS7799 certification, OECD security guidelines revision, the data protection directive and the government direct green paper.
- Advising the Society's officers on: The Society's professional codes of conduct; the necessary steps to be included in the ISM to cover security and appropriate nominations to be the Society's representatives on other bodies.
- We are working to create a register of Security practitioners which we hope will be operational in the summer of 1997 and assisting in the consideration of the register of consultants following the decision at the Society's AGM.
- We intend to establish an information bank as part of the Society's web site containing the official documents which security officers and auditors should be aware of. This site will also include the mechanisms for gathering

The Committee is expecting to be involved in the following areas in the coming year:

- Cryptography
- Security Evaluation
- Government Direct - Green Paper
- OECD Initiatives - cryptography & security guidelines
- Data Protection Directive
- BS7799
- Security of electronic commerce
- Commercial application of security
- Software quality as a security issue
- Domestic dependence on IT
- The Internet & Java programming language.

The Committee would welcome assistance from members of the CASG in two areas:

- Those who would be willing to participate in the work of the teams
- Identification of matters which members believe the Committee should be addressing.

If any member wishes further information about the Committee and its teams, or wishes to raise matters with the Committee they should contact J Williamson, the Secretary, at Benefield, Woodhall Lane, Ascot, Berks, SL5 9QW. Telephone: 01344 27956. Email: seccom@bcs.org.uk.

BCS MATTERS

Library Services for BCS members

By Hazel Roberts - BCS Librarian

My column is a little shorter than usual due to the fact that on the run up to christmas the IEE/BCS library does not seem to receive as many new books into the library as usual. The only exception to this are books on the subject of the internet and Java programming language which are new subjects in the computing world and are proving to be extremely popular to our users.

CASG readers will be pleased to know that we have received a few new book titles on the subjects of computer security which also includes Internet Security. Some of these titles may have been listed in previous columns.

0-387-94663-2
SLADE R
Robert Slade's guide to computer viruses: how to avoid them, how to get rid of them, and how to get help.
Springer, 2nd edition, 1996

0-7506-9600-1
CARROLL J M
Computer Security
Butterworth-Heinemann
3rd edition, 1996

0-8493-7179-1
WHITE G B, FISCH E A, POOCH U W
Computer system and network security
CRC, 1996

0-07-015841-X
DAVIS P T
Securing Client/Server computer networks
McGraw-Hill, 1996

1-56205-632-8
HARE C,
SIYAN K
Internet firewalls and network security
New Riders Press
2nd edition, 1996

0-471-13752-9
BERNSTEIN T, BHIMANI A B,
SCHULTZ E, SIEGAL C A
Internet security for business
Wiley, 1996

1-56205-557-7
ATKINS D, BUIS P,
IIARE C, et al
Internet security professional reference
New Riders Press, 1996

0-07-048215-2
PABRAI U O, GURBANI V K
Internet and TCP/IP network security: securing protocols and applications.
McGraw-Hill, 1996

1-855-54807-0
HUMPHREYS L
Security and the Internet: Rules for best practice
Blackwell-Science, 1996

Just to remind readers that the IEE/BCS Library catalogue is accessible via the Internet. The Institution of Electrical Engineers home page is at theWeb address: **http://www.iee.org.uk**

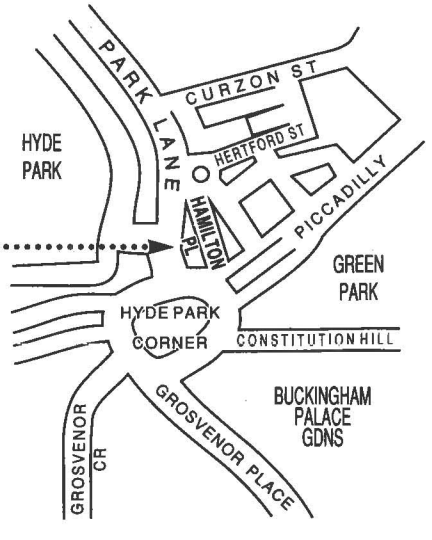
From the IEE home page you can find the library service details by clicking on the word library, this is a link to the library page. Alternatively, to connect immediately on to the library catalogue you can type in: **http://www.iee.org.uk/Library/Catalogue/Simple-search.html**

After searching for an item, the computer will ask whether you would like to place an order for that particular book, you must be a member of either the Institution of Electrical Engineers or the British Computer Society, a membership number will be required. Once the details of the book and your own personal details have been completed then the request is sent directly to the library desk for library staff to check.

Hazel can be contacted at the
IEE/BCS Library,
The Institution of Electrical Engineers,
Savoy Place, London, WC2R 0BL.
Telephone: 0171 344 5461.
Facsimile: 0171 497 3557
Email: libdesk@iee.org.uk

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ



casg
Computer Audit Specialist Group

British Computer Society

Management Committee

CHAIRMAN	Alison Webb	Consultant	01223 461316 amwebbcam@aol.com
SECRETARY	Raghu Iyer	KPMG	0171 311 6023 raghu.iyer@kpmg.co.uk
TREASURER	Bill Barton	BSkyB	0171 705 3000 bartonb@sky.bskyb.com
MEMBERSHIP SECRETARY	Jenny Broadbent	Cambridgeshire County Council	01223 317256 Jenny.Broadbent@finance.camcnty.gov.uk
JOURNAL EDITOR	John Mitchell	LHS - The Business Control Consultancy	01707 851454 jmitchell@lhs.win-uk.net
SECURITY COMMITTEE LIAISON	John Bevan	Audit & Computer Security Services	01992 582439
TECHNICAL BOARD LIAISON	Geoff Wilson	Consultant	01962 733049
	Allan Brown	Consultant	01803 872775 alan.brown@aduk.co.uk
TECHNICAL BRIEFINGS	Diane Skinner	Audit Commission	0117 9001418 diansk@globalnet.co.uk
	Jim Jackson	Lombard North Central plc	01737 776281
	Dave Cox	Lombard North Central plc	01737 776281
	Paul Plane	National Westminster Bank plc	0171 726 1882

Membership Enquiries to:

Jenny Broadbent
Room C309
Cambridgeshire County Council
Shire Hall, Castle Hill
Cambridge
CB3 0AP

Tel: 01223 317256

British
Computer
Society

PLEASE RETURN TO
Jenny Broadbent
CASG Membership Secretary
Room C309
Cambridgeshire County Council
Shire Hall
Castle Hill
Cambridge CB3 0AP

Membership Application

(Membership runs from July to the following June each year)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 members)* £75

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

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)* £25

INDIVIDUAL MEMBERSHIP *(A members of the BCS)* £15

BCS membership number: _____

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

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)