Editorial

The world of regulation is getting tougher. Each year the Government attempts to enact between twenty and thirty new statutes that effectively make you or your company a criminal in areas where you weren't so last year. On top of that the EU issues around twelve hundred new directives which, when subsumed into UK law have a similar effect. Then we have all the new regulatory requirements from such organisations as the Financial services Authority. Not to forget the voluntary stuff that we sign up to in the guise of ISO9000 and ISO17799. All in all there is a mountain of compliance to adhere to and the mountain is getting bigger each year. Turnbull got it right when he wrote that compliance was a key internal control requirement for organisations. Indeed, so great is the problem for those involved in information security that I have added compliance to the Confidentiality, Integrity and Availability triad. At least the acronym CIAC moves us away from apparently being an arm of a sinister secret service type of organisation, but more importantly it raises the profile of information security from being something that is 'nice to have' to being something that is essential to doing business. It's not uncommon these days to see IS auditor jobs being advertised with 'CISA or QiCA preferred' prominently displayed and soon IS security managers will be faced with 'CISM or CISSP required'. Likewise, contracts for supplying IS services will require 'ISO17799' accredited. In the world of regulation, having the appropriate qualification or accreditation will become a de rigour requirement for doing the work. This is because organisations, in order to show that they operate to best practice, will want themselves, or their staff, to be able to prove that they meet the appropriate regulatory requirement. So, if you expect to progress in the IS audit or security fields you will have to seriously consider obtaining a professional qualification. Even if you have an MSc in IS auditing, you will be forced to obtain yet another piece of paper to add to that already impressive list on your CV. So why is he banging on about qualifications I hear you ask?

The answer lies in the 'BCS Matters!' column of this Journal. Colin Thompson explains the new BCS membership structure, which has been partly designed with the members of its specialist Groups in mind. Many of you may think that you do not have the qualifications or experience to become a chartered MBCS member of the society and until now you may have been right. But the world is changing and as Colin explains, applicants for MBCS will now only need a maximum of 5 years ICT experience even if you hold no recognised academic qualification. The speed of processing has also been enhanced so you will not have to wait for ages after making your application. The fact that you are member of this group indicates that you probably work in the IS auditing or security field and as every letter after your name gives you an edge in the job progression game, I urge you to examine the new membership structure to see whether you are now eligible to become an MBCS .

Coincidentally, Bob Ashton in his 'Down Under' column reports on a situation where someone using the CISA designation had failed to do the mandatory CPE requirement and the designation had lapsed as a result. The need for qualifications to be checked at employment commencement is recommended in ISO17799, but as Bob points out there is no requirement to check that the qualification remain valid. Something to think about the next time you place an advertisement with a 'CISA preferred' sticker on it.

Our own Deputy Chairman, Alex Brewer, has crafted an article on programming using PERL, which as an old COBOL code writer I found particularly interesting. Open source is becoming a real competitor to the domination of Microsoft, so anything that raises its profile it to be welcomed.

The problems associated with the control of office applications, especially spreadsheets, is dealt with by Steve Semenzato. This is a timely reminder that no matter how well the main application is controlled the real risks lie with the use made of the data by the end user with the (usually) poorly controlled spreadsheet. Many of you will remember a survey by one of the big four that a third of the spreadsheets that they examined contained a material error so anything that can help in this area is to be welcomed.

How many times have you been told that your finding regarding a violation of your company's security policy is correct, but compliance is not immediately possible and therefore a waiver will be made? More times than you are comfortable with I expect. Gordon Smith tackles this subject with his usual verve and shows that ultimately the cumulative effect may expose the company to breaches of compliance legislation.

The problems associated with the control of office applications, especially spreadsheets, is dealt with by Steve Semenzato. This is a timely reminder that no matter how well the main application is controlled the real risks lie with the use made of the data by the end user with the (usually) poorly controlled spreadsheet. Many of you will remember a survey by one of the big four that a third of the spreadsheets that they examined contained a material error so anything that can help in this area is to be welcomed.

How many times have you been told that your finding regarding a violation of your company's security policy is correct, but compliance is not immediately possible and therefore a waiver will be made? More times than you are comfortable with I expect. Gordon Smith tackles this subject with his usual verve and shows that ultimately the cumulative effect may expose the company to breaches of compliance legislation.

Many auditors now get involved in special investigations where the evidential requirement is often higher than for normal audit work. Also, the investigation may require the evaluation of many different aspects of a situation which at first

sight bear no relation to each other. In order to help you in these situations I have arranged for a number of articles to be published in this and the next few editions that cover the various aspects of these investigations. In this edition we start the process with an article by Greg Krehel on the need to get your case into chronological sequence and another by Priscilla Emery dealing with the email archiving nightmare. These are complimented by Clive Carmichael-Jones' article on email forensics.

Jean Morgan, our Treasurer gives an update on our finances and also asks whether anyone is interested in tutoring a new MSc in Information Security that is being developed by the Open University. Now that would look good on your CV. Mark Smith has negotiated some substantial discounts on useful audit software packages. You will find details later in this edition, but the savings more than make up for your modest membership subscription.

I am off to Zurich for a week of conferencing. Well, someone has to do it!