Editorial

With this edition of the Journal you should also have received your renewal advice. There are five types of renewal: corporate main, corporate subsidiary, individual, student and courtesy. The corporate main member pays a subscription of £75 which includes up to four other people from the same organisation. Corporate subsidiary members receive notification that they do not need to take any action, although I highly recommend that they check that their main member is taking responsibility for payment. With transfers of staff and re-organisations it is easy to assume that action is being taken when it isn't! Individual renewals are of two types: BCS members and non-BCS members. The former pay just £15 while the non-members fork out £25. Full-time students receive a special low rate of just £10 to encourage them to take an interest in information systems risk management. Whatever your membership level, please take a moment to renew your subscription. Not only does this entitle you to editions of this Journal each year, but a scan of the list of either free, or heavily discounted events on the front cover should make you realise what a bargain this is. Subscriptions for other professional organisations often exceed one hundred pounds for a similar, or even lower level of benefits.

There is so much going on along the IT front these days that it becomes increasingly difficult to keep up to date. The dynamics of the technical, social, legal and business environments mean that there are now many fingers in the standardisation and qualifications pie. ISO 17799 requires accredited auditors, but what qualification(s) should they have? The BCS, in conjunction with the Information Systems and Control Association, is currently discussing the matter with one of the main ISO 17799 accreditation bodies. Starting from the presumption that the main role of audit is to provide assurance to senior management we then descend to the playing field of exactly what this assurance is and how should it be obtained? To my way of thinking there are two ways of approaching these questions.

First, what exactly is assurance? According to the various dictionaries 'assurance' is a guarantee, so immediately you see why the phrase 'reasonable assurance' tends to be used. We give a reasonable and not absolute guarantee that things are as management assert them to be. We cannot give absolute assurance without checking every transaction and 'absolute' becomes a nonsense word when we give any assurance over system development. So we settle for reasonable assurance. But what is reasonable? On what do we base the guarantee that we offer? This is where accepted audit practice and standards enter the equation. The audit profession is now well established and has a number of qualifications that indicate a degree of professionalism. CISA and QiCA are both basically saying that the holder has been found to meet a minimum level of competence. Compare this with the IT industry where the majority of participants have nothing that guarantees their professional competence. Before anyone tackles me with the 'I have a degree in computer science' argument let me make it quite clear that this is a measure of educational and not professional attainment. The BCS has only 39,000 members out of an estimated 650,000 people involved in the mainstream UK IT industry. Now let us examine the thorny issue of standards. The cynicism attached to these never ceases to amaze me. I recently addressed an audience of IT directors on the subject of IT governance. There was almost universal derision from the audience regarding the use of anything like ISO 9000, ISO 9126 or ISO 17799. Some even boasted of their manipulation of

ISO 9000 …… and these people were attending to find out about IT governance! When I challenged them on what other basis they should be measured against there was a singular lack of suggestions. So we are in a really strong position. We know that our main role is to provide assurance that IT is supporting the enterprise in a well controlled manner, We are professionally qualified (or should be) and we judge them against internationally recognised criteria. Throw in a bit of risk management and its game, set and match to us.

So what in this edition will enhance your knowledge even further? A survey of UK IT managers' views on security policies for starters, followed by an update from Australia on a recent survey there on computer crime and a sad story about stupidity. Colin Thompson provides his usual informative guide on what's happening at the BCS. As a result of the AGM you are now represented by a newly constituted Committee and a number of them have taken the opportunity to introduce themselves in this edition.

I hope that you have a good break and look forward to seeing you at our meetings in the Autumn.