

Editorial

John Mitchell

It's hard to believe that it was as long ago as 1965 that some far sighted individuals created the Auditing by Computer (ABC) specialist group of the BCS. Now, forty years on, the Information Risk Management and Audit (IRMA) specialist group is its direct descendent. During that time there have only been a handful of chairman; Ron Middleton, William List, myself, Alison Webb, John Bevan and currently Alex Brewer. We are the oldest, continuous specialist group in the Society and as we enter our ruby anniversary I believe it not unreasonable to reflect on the changes that have taken place since the Group's formation.

Mainframe computers ruled the roost for the first twenty years. Slowly developing from a single program capability to multi-tasking leviathans. The very first computer that I can remember was an Elliot 808 with paper tape input. I was introduced to it on a school visit to London University in the mid 1960s. I played tic-tac-toe (a kind of noughts and crosses game) against it and lost. In those days you were required to have two Advanced levels, one of which had to be in mathematics to even operate a computer! My first work machine was a CDC 3200. The 3200 reflected its memory of 32k bits. It had eight tape drives which used 2,400 feet reel to reel serial tapes, an 80 column punched card reader, a line printer which used continuous paper and a teletype for operator-to-machine communication. Initial Program Load (IPL) "booted" the operating system so that the single application could be loaded. This was the machine on which I cut my operating and programming (COBOL) teeth. An eight-tape sort in a darkened room was a sight to behold. The flashing lights on the tape drives, coupled with the whirring of the reels were the stuff of science fiction and I was part of it!

During the early 1970s I graduated to a CDC 6400 (twice the memory), then through the IBM 360 and 370 ranges, Univac's 1100 series and onto Honeywells and ICLs. The early ICL machines (1902s, 1903s and 1904s) used the George 2 operating system, but then ICL developed VME/B which was built with security in mind from the ground up. I remember that the VME/B High Security Option received an unprecedented B1 security rating from the American Department of Defence, at a time when security was a cumbersome bolt on extra for the IBM MVS operating system. I generated and implemented a CICS teleprocessing system and got to grips with network protocols, dumb terminals and fixed drum storage and exchangeable hard disks. I audited hierarchical databases, such as IMS-X and made a small name for myself by writing an audit programme to guide other auditors through the torturous process of gaining assurance that it was well controlled. I used Filetab and Easytrieve for my interrogations and found some amazing things, such as the £9 billion asset, the £6 parcel of land and incorrect depreciation and age of debt calculations. I was edging my way onto the international conference circuit by flying the then novel idea of looking at the data to identify control deficiencies rather than using the resource intensive system

based audit approach. I applied the second law of thermo dynamics to data integrity and found that it worked quite well.

Meanwhile, mid-range machines in the form of PDPs and VAXs were coming through, but I couldn't take them seriously until the IBM Series 3 and later the IBM 400 came on the scene. Then in the late 1970s the dawn of the microcomputers, in the form of Commodores, Apricots and Superbrains (really), which used the CP/M (Control Program for Micro-processors) operating system heralded the move to what we have now. The dominant operating system became MS-DOS which transformed into the Windows we know today. During that time I moved away from COBOL and into relational databases such as dBase, which gave me a grounding in Oracle and the visual languages. However, what I learned in my mainframe education stood me in good stead for what we have today and will have tomorrow.

This Group grew with along with the technology and at its largest we had well over 500 members, but we lacked, and still do so, an essential requirement of a professional body; a qualification. This has left us vulnerable to other professional bodies, such as ISACA, which offers its CISA and CISM qualifications.

During my 25 years with the Group I have met some marvellous people who have moved computer auditing from an art form to a science. We drank more alcohol in those days (it was socially acceptable) and so did the IT crowd. If you wanted information, then the interviewing technique involved taking the systems programmer to the local pub and drinking him/her under the table. The technique may be questionable, but it still beats the hell out of flowcharting the system! I find that today's computer auditors take themselves far too seriously, but then we tend to be better qualified now than the IT people. We have MIIA, CISA, QiCA, CISM and CISSP to mention just a few and most computer audit jobs require one of these, whereas the IT lot are mostly professionally unqualified (for example, only a small percentage are members of the BCS). This really should give us an edge, but I still see computer auditors on the defensive when dealing with the techno gabble of the IT people and I still see SLAs written from the point of view of the supplier rather than the customer. My red pen comes out as I try to turn these into business speak and to identify the associated metrics. IT governance is primarily about measurement. "If you can't measure it, you can't manage it", is my motto, but determining the relevant metrics is not easy. I am reminded of what John F Kennedy, the young President of the USA in the 1960s said. "We do these things not because they are easy, but because they are hard". Easy measurements tend to be useless from a governance viewpoint. After all, how do you measure the value added of IT to the business? Well, I have a few solutions, but commercial confidentiality prevents me from sharing them with you. After all, I have to eat too!

However, reading this journal can help you to move closer to solving that problem. Vasilis Katos from Portsmouth University provides an insight into how you can apply mathematical techniques to obtain optimum network configuration. Jack Vivret discusses the implications of the Freedom of Information Act and Bob Ashton describes the Australian approach to dealing with trans-national high tech crime. Mark Smith details the benefits he has negotiated for you and Colin Thompson updates us on the activities of our parent body. Happy reading.