Editorial

When I did my doctorate in risk management back in the mid nineteen eighties I found very few organisations, outside of the insurance sector, that linked business objectives to risks to controls. When I set up my own business in the late nineteen eighties I faced an uphill task in persuading senior people, especially heads of internal audit, that business, whether for profit or not, was all about managing risk. Indeed, the only reason that we have controls is to manage risks so you would have thought that heads of internal audit would have been able to make the link. Not so. The general response was along the lines that "we've always audited payroll on an annual basis and that's what we will continue to do". Even with the advent of Turnbull there is still a misunderstanding by many heads of audit on the link between critical success factors, key goal indicators and key performance indicators. No where more so is this true than when they consider information technology. Now, the only reason we have all that hardware and software is to aid the management of data to aid decision making. It therefore makes sense for the IT audit programme to be aligned with those risks that may impact on the confidentiality, integrity, availability and compliance of information technology in the management of the entity's data. Indeed, if this approach is used the IT auditor will notice how easy it is to decrypt the complexities of the technology to simple business needs. For example, we have virus protection to help preserve the integrity of our code and data. Now even senior management can recognise that spending money in this area is a good thing.

I recently conducted an audit of e-commerce availability for a UK based company with world-wide operations. They had decided that their strategy was to provide a web based service to their 600,000 or so customers and that one of the critical success factors was the availability of the service to their customers at time of need. Taking this as their starting position I helped them to identify two key risks that would prevent the achievement of this business objective. In simplistic terms these were:

- *Customers are unable to access the system leading to them being unable to place orders resulting in loss of income*

- *Customers are unable to obtain help with non-availability problems leading to dissatisfaction with the company resulting in complaints, adverse publicity and loss of customers.*

Eighteen root causes (15 relating to availability & 3 to support) that could lead to these risks crystallising were agreed with the company. These were risk assessed at the inherent level (i.e. before any controls are applied) and subsequently at the residual level (i.e. after controls are applied). Any root causes that were considered not to be sufficiently mitigated resulted in an improvement plan being created and agreed with relevant staff.

Now e-commerce availability is a technically complex subject, but by using a risk based approach it was not only possible to focus on the important areas, but I was able to explain these to management in the context of impact on business objectives, which they intuitively could understand. More importantly, from my point of view, I was able to concentrate my resources on those areas that were really important and complete the job quickly while achieving a high standard of work.

I have been using this approach for a number of years now and it is gratifying to see the impact it has on my clients. Once their eyes are opened there is no going back and they often change the approach of the entire department, because if it's good enough for IT then it must be good enough for the rest of the organisation. So I urge you to give it a try. Your audit planning and work will never be the same again and it will be for the better.

Which has just reminded me of a sign that I once saw above a bar in the Balearics; "Try our sangria. You'll never get better". Oh well, I am sure the intention was right. A bit like many auditors current work plans. The intention is right, but the implementation needs some serious enhancing.

On that issue, the main article in this edition relates to risk management and the use of computer assisted audit techniques. The author, Effrosyni Papaefstathiou (Froso for short), is a Greek national who did her MSc in internal auditing at City University's Business School. City was the first university in the UK to have a post graduate programme dealing with internal audit and it was my alma marta for my doctorate. Much of the original teaching team are still in place and they attract students from across the world, so I am always pleased to maintain my links.

We also have a piece from Gordon Smith the CEO of Canaudit who examines the implications of outsourcing on a nation's critical infrastructure. The article concentrates on the USA, but its implications for the UK are the reason that I include it here. Well do I remember taking Michael Portillo to task when, as Minister for Defence, he outsourced our armed forces payroll to EDS, an American firm. Since then EDS has taken over the running of almost every government computer system so I am as one with Gordon on this particular issue.

We also have our usual round up of BCS matters from our parent body's Deputy Chief Executive, Colin Thompson (no expense is spared by me in reaching the top echelons of the Society), who explains the important changes to the BCS membership structure and how this will benefit IRMA members who are not currently members of the BCS. We also have a report from our Treasurer, Jean Morgan, on the state of our finances (very good it appears), some information from the antipodes from Bob Ashton our Australian correspondent and a monster humour section to get you through the Christmas festivities.

As a Christmas treat we have also negotiated some excellent deals for IRMA members with some software suppliers. See Mark Smith's column for details of the savings that you can make. On that I leave you with the compliments of the season and your Committee's best wishes for a very happy and prosperous new year.