IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL
volume 14 number 1 winter 2003 ISSN 1741-4229

Programme for members' meetings 2003/2004 season

Tuesday 21st October	**WIRELESS NETWORKING UPDATE** Things are moving rapidly in the wireless networking world. First a quick round up of what is happening in the wireless world, and then a look at changes to fix the security issues which have dogged this technology since it was introduced.	Late Afternoon
Tuesday 25th November	**E-MAIL MANAGEMENT AND SECURITY** Vogon International	Full Day
Tuesday 2nd December	**PDAs AND MOBILE COMPUTING RISKS** Shirt-pocket sized computers are many times more powerful than mainframes of just 20 years ago. Many can store hundreds of Word documents, Excel spreadsheets, PDFs and the like. Laptops can be many times more powerful still, with massive hard drives. They frequently have weak security. Yet these devices often contain sensitive information and many are linked to corporate systems.	Late Afternoon

2004

Wednesday 28th January	**COMPUTER AUDIT BASICS, PART I**	Late Afternoon
Tuesday 17th February	**NETWORK MANAGEMENT**	Full Day
Tuesday 16th March	**OUTSOURCING**	Full Day
Tuesday 11th May	**SERVER FARMS** **AGM precedes the meeting**	Late Afternoon

Please note that these are provisional details and are subject to change.

The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.
For venue maps see inside back cover.

Contents of the Journal

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should be by e-mail and in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality electronic digital image.

Submission Deadlines

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

The ***Journal*** is the official publication of the Information Risk Management & 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
Email: john@lhscontrol.com

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by PostScript, Tring, Herts.

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 help 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. 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 mata 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.

John Mitchell

Letter to the Editor . . .

John Mitchell
BCS IRMA

3 November 2003

Further to your Editorial in the IRMA SG Journal Vol 13 No. 4, I was moved to write and advise you of my involvement with the ECDL and my attempts to improve the security awareness content of it.

I put a proposal forward to the original founder of the ECDL in November 2000, providing in detail both content suggestions and the reasons why a more in-depth Security module should be incorporated. The "founder" just happens to be my father! My proposal was forwarded to the current Managing Director of ECDL in Ireland and I understand that there is a "two horse" race between my proposal and one from Sweden. The influence of the European Commission and the nature of the birth of the ECDL mean that the channels through which change may be realised move very slowly indeed, apparently. It is interesting that the origination of the ECDL remains in the pure world of IT/technology, as opposed to the humanistic world of the regular user who really needs

At the time of my original proposal (finalised in February 2001), the main content suggestions focused on providing information in the following areas:

- What Information Security is and why it matters
- What the relevant Legal Issues are
- What your personal and management responsibilities are
- What the appropriate behaviour is
- What the various basic elements of a good information security management system are made up of.

These could obviously be expanded upon quite easily – and made relevant for both national (UK) and international audiences alike. As I am currently undertaking the ECDL myself, I am getting first hand experience of what it means and how it is structured and a separate Security Awareness focused module would be of tremendous use and value to all candidates. Having spent the weekend setting up a laptop for a family member who is now at University, it was interesting to meet head-on the first question of "What's a firewall?" when loading the Norton Security 2004 programme……. There's quite a way to go in terms of education at all levels and more needs to be done at school level too.

Andrea Simmons, AMBCS
BCS IRMA & ISSG member
Simmons Professional Services Limited

ENTERPRISE RISK MANAGEMENT: THE NEW APPROACH. WHAT IS THE ROLE OF THE INTERNAL AUDITOR & COMPUTER ASSISTED AUDIT TOOLS & TECHNIQUES?

EFFROSYNI PAPAEFSTATHIOU

INTRODUCTION

This paper presents a study of the relationship between internal auditors and the risk management process. It refers to the change from the control-based auditing approach to the risk-based auditing approach. This change derives from the current state of the business environment which is characterised by volatility, competition and instability. The Turnbull report states clearly that a company's internal control system has a key role in the management of the risks that are significant to the fulfilment of its business objectives, contributing to safeguarding of shareholders' investments and the company's assets. The new role of the internal auditor also becomes apparent from the new definition of internal auditing as defined by the Institute of the Internal Auditors. This demonstrates clearly that the internal auditor has a clear and critical role in the evaluation and the improvement of the effectiveness of the risk management process. Selim and McNamee (1998) have stated that there is a definite emerging paradigm shift from a control-based internal auditing to a risk-based internal auditing among leading practitioners. Both internal auditing and risk management are co-evolving with the ascendance of global business risk as a major corporate governance issue.

The evolution of the audit profession has not only encompassed the new risk based approach, but also to the widespread use of technology to perform the audit work. The revolution that technology has brought in any aspect and any field of our day-to-day life and business practice is certainly obvious. Internal auditing activity could not stand away from this.

Computer assisted audit techniques (CAATs) are now playing an undeniable and significant role. The traditional manual approach is not enough anymore. Use of the technology becomes a necessity, but we have to consider this necessity not as a liability, but as an advantage. CAATs can be used to provide credibility, to transform manual operations into automated audit, with resulting saving of time. CAATs can also be used in the risk assessment process.

This paper will try to explain the nature of the business risk, mainly at a strategic level, the risk assessment methodology that is currently used by the companies and also how do they perceive the risk management process in general. All these aim to provide a description of the approach of companies to risk management, so as to discover any inefficiency, as far as is this is possible. Another objective is to describe the role of the internal auditor in risk management, how can he or she help, at which stages, which factors should he or she should consider and so on. The above can be summarised into the following questions:

1. How does business manage risk?
2. How does the internal auditor participate in risk management?
3. Do they use CAATs? How do they use them?
4. If they do not, why not?

ENTERPRISE RISK MANAGEMENT – THE NEW APPROACH

1.1 Evolution Of The Audit Profession

The speed of change is accelerating in all fields: economic, technological, social and political, inside and outside of the organisation and beyond its ability to predict the future and measure the impact. The scene for internal auditing is also changing and internal auditing has followed the pace of change and become involved in the new challenges. The traditional approach was focused on planning, verification and reporting. Later, compliance auditing was adopted and the organisation was split up into separate functions and/or business units. Each function–transaction was part of a "cycle" in which could be grouped for example revenues, expenditures, production etc. For each cycle, control criteria were identified and against those criteria tests were performed to assess the effectiveness of the control system (Chambers et al., 1987). But this approach has many limitations. Auditors work only on existing systems and processes, evaluate past performance, follow a predetermined schedule that leaves no room for innovation and creativity.

Systems-based auditing took the place of the traditional approach. "Systems-based auditing is a top-down structured approach to the assessment of controls within an organisation and its operations. The prime purpose of a systems audit is to evaluate the extent to which the controls in an activity can be relied on to ensure that objectives are met and risks are effectively managed" (Wade, 2003). Systems-based auditing concentrates on significant systems and not on routine transactions and low-level activities. By focusing on the whole business system and not the individual parts recognises the interaction among the smaller business systems and their effects on the entity and tries to identify the causes rather than the symptoms. The benefits are considered long-term, because controls are directed to the prevention of future problems instead of detecting past mistakes and the controls are established in accordance with the business objectives and risks. The new approach has created a new role for the internal auditor, instead of detector and checker; Internal Auditor became an assurance provider, assistant and teacher.

The current business environment is characterised by volatility, strong competition and uncertainty, causing the increase of risks encompassing business activity. Along with this unstable environment internal audit activity changes its focus from control-based to risk-based. Internal auditors adopt a proactive approach rather than reactive, broaden the scope of internal auditing and attempt to provide high value for the cost of service. They undertake wider responsibilities and change their focus from past performance to assess the company's future prospects and risks.

This definition of internal auditing creates a new role for internal auditor, the one in risk management. Responding to the business needs "there is a definite paradigm shift from control-based internal auditing to a risk based internal auditing. Managers are operating in an increasingly complex and global environment and risk is a central element of corporate governance. The emergence of risk management as a key organisational process gives the internal auditing profession a unique opportunity to shift its focus to risk" (McNamee & Sellim, 1998).

Internal auditing has raised its standards and is placed on a strategic level within the organisation by becoming a "future-orientated, independent and systematic evaluation of the activities of all levels of management" (Chambers et al., 1987). The profound changes in technology forces internal auditors "to provide assurance not only about the information, but also the security and protection of critical infrastructures on a global basis" (Le Grand, 2002). Communications skills, thorough understanding of management principles, challenges and impacts of technology on management and organisations, critical thinking on the use of computer software to perform audit activities, efficient and organised development of communication are only some of the prerequisites that the internal auditor should acquire or improve in order to face the challenges rising by the increasing speed of business progress.

1.2 Nature of Business Risk

Progress has been achieved because there were people with visions and willingness to go forward, to pursue goals, usually without being able to predict failure or success. The same principle applies to organisations. Organisations exist to achieve their goals for growth, return and profit generation. Unfortunately, they have to operate within a risk framework, which enhances the potential for failure.

"Risk has been defined as the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood. Risk may be considered in terms of outcomes as a possible outcome which cannot be predicted with certainty and which would be unwelcome because it would be counter-productive" (Chambers, 2002).

The main feature of risk is uncertainty and this makes risk complex, intangible, widely and constantly variable subject. Uncertainty is what contributes to the improvement of knowledge, because it represents the gap between what is known and what needs to be known to make correct decisions. Dealing intelligently with uncertainty and consequently with risk is not the alternative to responsible business decision, it is of it (Mack, 1971).

The major categories of risks as defined by the Enterprise Risk Management Committee of the Casualty Actuarial Society are the following (CAS ERM Committee, 2003):

Hazard Risks include risks from:

- ❏ Fire and other property damage.
- ❏ Windstorm and other natural perils.
- ❏ Theft and other crime, personal, injury, business interruption.
- ❏ Disease and disability (including work related injuries and diseases), and
- ❏ Liability claims.

Financial Risks include risks from:

- ❏ Price (e.g. asset value, interest value, foreign exchange, commodity).
- ❏ Liquidity (e.g. cash flow, cal risk, opportunity risk).
- ❏ Credit (e.g. default, downgrade).
- ❏ Inflation/purchasing power, and
- ❏ Hedging/basis risk.

Operational Risks include risks from:

- ❏ Business operations (e.g. human resources, product development, capacity, efficiency, product/service failure etc.).
- ❏ Empowerment (e.g. leadership, change readiness).
- ❏ Information technology (e.g. relevance, availability), and
- ❏ Information/business reporting (e.g. budgeting and planning, investment evaluation etc.).

Strategic Risks include risk from:

- ❏ Reputation damage (e.g. trademark/brand erosion, fraud, unfavourable position).
- ❏ Competition.
- ❏ Customer wants.
- ❏ Demographic and social/cultural trends.
- ❏ Technological innovation.
- ❏ Capital availability, and
- ❏ Regulatory and political trends.

Categorising risks is an important issue for two main reasons:

1. It helps the organisation to identify existing and potential risks, and
2. It can be used to collect information about the risks that the organisation is exposed so as to create a risk profile.

Risk assessment is the first step in the risk management process, but it requires that useful categories of risks have already been developed. There are some standards categories like those that have been already mentioned before (hazard, financial, operational and strategic), but categorising of risks also depends on the type of industry, sector, size of the business etc. For that reason, the enterprise should be flexible and observe the environment in which it operates so as to develop meaningful and related measurement scale.

A survey that was conducted by AON and entitled "THE AON EUROPEAN RISK MANAGEMENT AND INSURANCE SURVEY 2002-03" collected information about the risks that pose the greatest threat to business:

Table 1: GREATEST RISKS FACING BUSINESS

Business interruption	1
Loss of reputation	2
Products liability/Tamper/Brand reputation	3
Physical damage	4
General liability	2
Employee accidents	6
Failure to change/adapt	7
Environmental pollution	8
Professional indemnity	9
Failure of key strategic alliance	10
Directors' and officers' liabilities	11
Employee recruitment/retention	12
Computer crime	13=
Other crime	13=
Political risk	13=
Environmental sustainability	16
Terrorism	17

Source: THE AON European Risk Management & Insurance Survey 2002-03 Greatest Threats

Based on the information of the survey, loss of reputation is considered as the second most important to business interruption. Nevertheless, only 22% of companies have established a formal strategy to face that risk. In addition, professional indemnity represents a major concern for the UK respondents, whereas environmental risks are classified as a high priority for the rest of the European countries. Finally, despite the latest terrorist events, companies do not seem to consider political risk and terrorism as a major threat to their business.

Risk is measured in terms of probability (or frequency) and severity (impact). Risk measurement has a crucial role in the risk management process and provides the basis for evaluating and selecting risk control and alternative solutions (Banister, 1997). The special task in risk measurement is that some risks are relatively easily to be quantified. For example, the impact from a fire on assets, but there are risks like the reputation risk or the loss of intellectual capital, which cannot be quantified by using statistical formulas or financial models. In this case the risk manager should try to identify and evaluate all the relevant factors that influence the specific risk and try to cover all the aspects of the potential occurrence of the specific risk so as to make a reasonable estimation.

It is worth mentioning that many risk assessment practices are and based on the assumption that there is an inverse relationship between frequency and severity, so that big losses are infrequent and small losses are more frequent. This is not a constant relationship and it is different for different types of risk (Banister, 1997). Additionally, many likelihood ratings are based on the assumption that because something has not happened in the past it will never happen in the present or the future. Unfortunately such a belief might be dangerous, because threats to the business can come from any direction and sometimes losses are occurred by a risk that never occurred to anyone.

Recently risk management has become a focal point within the business environment. Financial scandals and collapse (Enron, Marconi) have drawn attention and can be attributed to failures of risk management. Publications by professional bodies like the Turnbull report emphasises the responsibility of senior management and the board for a sound and effective internal control system that addresses and manages risk adequately. Apart from the increased attention on risk management, a major change has occurred in the treatment of a variety of risks. Organisations are avoiding treating risk as being separate from their strategy and attempt to adopt a more holistic, comprehensive and forward-looking approach to risk management.

The overall evolution toward strategic risk management or Enterprise Risk Management as it has been named can be affected by a number of driving forces (CAS ERM Committee, 2003):

1. **Increased complexity of risks**
   Globalisation, complicated financial systems, accelerating pace of business, greater customer expectations and advance of technology contribute to the growing number and complexity of risks.

2. **External pressures**
   Regulatory authorities, stock exchanges, institutional investors, rating agencies (e.g. The Moody's) and corporate governance bodies (e.g. the Combined Code in UK, the KonTrag in Germany, the AS/NZS 4360 (1995) Risk Management, which is the first official standard on risk management developed by the joint Australian and New Zealand technical standards committee) point out that senior management should take greater responsibility for managing risks on an enterprise-wide scale.

3. **Portfolio Point of View**
   The framework in which Modern Portfolio Theory operates provides concepts that can be applied beyond financial risks and include risks of all kinds. A number of principles derived from this framework:
   - ❏ Portfolio risk is not the simple sum of the individual risk elements.
   - ❏ To understand Portfolio risk one must understand the risks of the individual elements plus their interactions.
   - ❏ The portfolio risk or risk to the entire organisation is relevant to the key risk decisions facing that organisation.

   Those principles influence the practice of ERM and recognise the fact that "risks must be managed with the total organisation in mind".

4. **Quantification**
   Quantification of risks in terms of impact and likelihood has become easier due to advances in technology and expertise, even for those risks that have been historically difficult to quantify due to their infrequency and unpredictability.

5. **Benchmarking**
   Exchange of information, common ERM practices and tools among organisations enrich the context of ERM and promote further development.

6. **Risk as Opportunity**
   Over time and with practice, organisations have become more capable and expert on managing the risks. Access to sources of information about risks characteristics gives the opportunity to evaluate promptly the impact of the various exposures and create more complete risk profiles. Investment organisations offer opportunities to organisations to hedge their positions and protect themselves against financial and hazard risks. All these reasons have contributed to a different attitude towards risk. Organisations recognise that fact and actively pursue other risks can offer opportunities for creating value, along with the traditional strategies for mitigating or eliminating risk exposures.

1.3 Organisational Practice in Risk Management

Risk is about uncertainty on plans and decisions. Organisations are trying to manage their operations in such way so as to mitigate, eliminate or transfer risk. Less often they try to pursue risks, when risk is seen as an opportunity for greater profit. Given the fact that the environment is constantly changing, part of that change is also the customers' needs. The challenge for organisations is to manage risk with the less harm or loss for them, meet their customers' needs and gain competitive advantage.

The nature and implications of risk has changed the attitude of organisations towards risk itself as a concept and also to the way of treatment of it. Until recently, the approach of most companies to risk management was to assign different risks among functions and operating units and placing the risk

management process in a medium management level. This "silo" approach as it has been named - "management segregated among operations or by specific risks" (CFO, 2002) has lead to treat risks as being separated from the organisations objectives and without taking into consideration the interaction among risks. For example, each division might look after its own risks, managing foreign exchange in treasury, hazard risk in the insurance department and business risks in the planning function (CFO, 2002).

In summer 2000, Arthur Andersen held risk workshops involving 100 heads of Internal Auditing, risk managers, company secretaries and others working in risk management in top U.K. companies giving them the opportunity to discuss a their experiences and opinions. The message from the meeting was that the "Turnbull report has been widely accepted as a compelling impetus for risk management. Unless risk management becomes more than an act of compliance, companies are unlikely to reap the real business rewards on offer" (Teji et al., 2001). Since then and until now the challenge is to get risk management an integrated part of the business operation, exploit the linkages with the business strategy and embed a new way of thinking about risk into processes and decisions. The following chart (figure 1) shows the progress that organisations make, as they become more sophisticated and expert at managing risk. At the initial stage, risk management activities have been assigned to specific individuals and the efforts are concentrated on identifying the risks. At the next stage, risk management becomes repeatable; there are available dedicated resources and a common language. At the defined stage, risk management has become a defined process. Responsibilities for risk management and for consistent reporting of risk are defined clearly. The managed level means that risks are identified and managed within the enterprise context and the interaction between all the kinds of risk is recognised. At the optimising stage risk management has been integrated into business planning process.

A discussion with the workshop participants regarding the figure below has provided evidence about the position of the organisations. These early results suggested that there is a gap between where the organisations were and where they wanted to be. The findings of those workshops were not only that they proved the need for Enterprise Risk Management and the fact that is not an obligation but a necessity and a ambition of the organisations to be better protected from the external and internal environment.

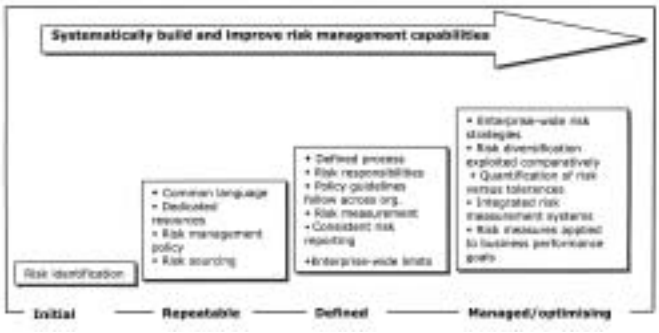


Figure 1: "Where is your company?", Arthur Andersen Workshops-Summer 2000

Source: TEJI, T. & KETTEL, M. Mastering risk beyond Turnbull, ***Internal Auditing & Business Risk****, March 2001.*

The CAS Committee on Enterprise Risk Management has adopted the following definition of ERM:

> "Enterprise Risk Management is the discipline by which an organisation in any industry assesses controls, exploits, finances and monitors risks from all sources for the purpose of increasing the organisation's short-term and long-term value to its stakeholders."

The definition recognises that ERM is a discipline, which means that there prescribed and defined procedure, which applies to every type of industry. It also points out that risk management activities should be directed to every potential source of risk and not only to the hazard and financial risks, where insurance industry is traditionally concentrating. The definition also places importance to the corporate responsibility towards the stakeholders.

In October 2001, CFO (Chief Financial Officers) Research services (a unit of CFO Publishing Corp.) conducted a survey sponsored and published by AON. AON is a global risk management, insurance brokerage, reinsurance, and human capital consulting services company (**http://www.aon.com**). The research was conducted in USA and Europe and attempted to describe how companies align risk management and their strategic goals[1]. In addition, Tillinghast carried out a similar survey[2]. This was a global benchmarking survey on Enterprise Risk Management and records how companies are starting to adopt the new approach to risk management in the insurance industry (Tillinghast Towers-Perrin, 2002a). Tillinghast is a division of Towers-Perrin a global management consulting services firm and it provides actuarial and management consulting services. It has worked together with The Institute of Internal Auditors Research Foundation and the Conference Board of Canada to prepare an in-depth monograph on the key success factors and the benefits of Enterprise Risk Management (**http://www.tillinghast.com**). Although the survey focuses on the insurance industry which may be considered as a restriction on the justification of the results for the whole business community, the results of it agree with those of the survey conducted by the CFO Research Services, in which different types of organizations participated, such as ABB Financial, Akzo Nobel, Aventis, Corning, Danone, Duke Energy, Novell and others. Some of the major results follow:

■ Both surveys have shown that managers are dissatisfied with their risk management techniques, processes and tools and experienced challenges in implementing ERM. Only 5% of the survey respondents from USA and about 1% from Europe are very satisfied with their current approach to risk management ("silo" approach"). The respondents from both regions, North America and Europe, share the same degree of satisfaction, about 40%, the current risk management practices of their organisations effectively support their business objectives.

■ Almost half of the respondents declared that they have already partly integrated risk management across their organisation. The other half treat risks in separate functions, but 40% of them predict that in three years they will have integrated risk management fully across the organisation.

■ The more risk management is integrated to the organisation and risks are managed by adopting a holistic view, the more closely the strategic risks are aligned with the risk management practices. In other words, CFOs are more satisfied when risk

[1] Strategic Risk management – New Disciplines, New Opportunities (CFO, 2002).

[2] Enterprise Risk Management in the Insurance Industry, 2002 Benchmarking Survey Report.

management is fully integrated across the organisation, because risk management is tied to strategic planning, and thus it is more effective.

■ Although the previous results show that there is serious progress in implementing ERM, only 15% of the respondents have a Chief Risk Officer (CRO) in place and only 5% are planning to appoint a CRO in the future. Appointing a CRO is considered an effective solution in terms of transmitting the message of change, establish a common language and bring the various functions together.

■ Audit committees should be actively involved in risk management and together with a risk committee can have an overview of the whole process, ensuring that all major risks are addressed adequately and managed effectively. Seventy three percent believe that audit committees should be more involved in ensuring that risk management is aligned with overall business strategy.

■ Organising risk management across the organisation can evolve to competitive advantage. Better capital allocation, better management of the risks than competitors will strength the financial situation and provide better returns, satisfying the regulatory authorities for a healthy financially organisation and an organisation that provides payback to the shareholders.

■ Implementing ERM is not a simple task, because there are several obstacles that prohibit its successful implementation, such as the existence of a common risk terminology, cultural barriers, lack of uniform metrics and inadequate IT systems.

■ Nothing can guarantee success, there is no secret way and there is more than one way to the achievement of goals and the objectives.

1.3.1 Benefits Derived from Enterprise Risk Management

As previously stated many organisations are determined to adopt a broader and more forward looking approach to risk management. The objectives and consequently the benefits from ERM may vary by industry, but from that an overall picture can be drawn. It has been observed that the shift from the "silo" approach to a more holistic approach, provided by ERM, is not only a response to the regulations, but also because organisations have recofnised that ERM is good business practice, providing them with the opportunity for a coherent conceptual framework for managing risks holistically (Tillingast, Towers-Perrin, 2002a). Even more, it drives the decision maker to find ways to increase shareholder value. Apart from the improvement in achieving traditional goals, such as better risk prevention and more effective reporting of operational risk issues to senior management, it is believed that Enterprise Risk Management can offer to the organisation various benefits (CFO, 2002).

1. Improved response to the full range of risks.

Integrating risk management and planning leads to improved response to the full range of risk. Effective risk management means that the full range of risks should be recognised.. Risk assessment workshops and interviews will provide details about the full picture. Strategic risk management also requires effective communication channels and a fully developed reporting line to be in place. Quantification of risk is also a significant issue, so that risk levels in different units can be compared and aggregated. The survey by the CFO regarding the risks that the companies quantify has revealed several areas that are inadequately measured. Each industry confronts some specific risks that are relevant to its business activities and it is likely to measure those risks, but there are also companies that are unable (or do not try) to quantify their industry's major risks. For instance, although the risk of data interruption is recognised as a major risk by the financial services firms only 12% of these companies measure this risk (CFO, 2002).

2. Better capital allocation

By aggregating risks, management has the opportunity to gain in-depth and complete knowledge of the risk concentrations. Adequate appreciation of the risks will provide senior management with an accurate sense of the total risk each business unit carries. A comparative analysis of the risks and opportunities that each project or new initiative has will support the decision making process positively and help to allocate resources effectively. Capital allocation decisions will be managed more efficiently because they are based on the risk-return characteristics of each project derived from the organisation's entire portfolio view instead of the "silo" approach (Elliot, 2001).

3. Earnings' growth

ERM is not only about identifying and mitigating risks, it is also a formal and systematic discipline that enables companies to have a clear picture of the risks associated with the company's various earnings streams. Information about the risks that growth strategies e.g. mergers, acquisitions and distribution channels bring, enables companies to make more reasonable decisions and produce the best return. Strategic risk management facilitates a complete appreciation of the risks, which enables managers to see them within the portfolio context and project the firm's overall earnings volatility. The impact of unexpected events can be avoided or mitigated and potential financial losses can be reduced.

4. Competitive advantage

Many companies believe that risk management can create competitive advantage for them. First of all, adopting a holistic view to risk management will assist the organisations to manage risk better than their competitors and will direct their activities to more profitable decisions because the project's risks are evaluated more thoroughly. Integrating risk management within the Modern Portfolio Theory will facilitate the recognition of good investment and improved performance.

1.3.2 Barriers to the Implementation of ERM

According to the respondents of the CFO survey, implementation of Enterprise Risk Management has to overcome some obstacles, before it starts to produce results.

1. Lack of uniform metrics across the organisation

Organisations that participated in the survey by the CFO magazine recognised that one of the most significant barriers to the implementation of ERM is the lack of uniform metrics across organisations. Uniform metrics are necessary because a common set of risk definition and terminology and a common language has to be in place together with a communication line to transmit the results of each stage to senior management. Although for some companies, for instance financial firms, is easy to quantify their risks, this might be difficult for other kinds

of businesses. Risks like those related to the loss of intellectual capital or the damage to reputation are not easy to quantify. A uniform metric, which would incorporate all risk, would benefit the organisation.

2. Too much time required for design and implementation.

Implementing strategic risk management is not a simple process, it requires time for each company to evaluate and decide what type of strategic risk program it needs and how much time it requires to implement the full program. Practitioners stated that the total period is about three to four years and probably more until the first positive results appeared. Within this long time frame support from senior management and full awareness of the board of the benefits, such as cost savings and better management of the previously neglected risk will enhance the possibility for successful implementation. A solution to this practical problem could be that the company might implement the project in stages or focus on a specific business unit.

3. Incompatibility with corporate culture

Generating a holistic enterprise-wide risk management has proved to be a hard task. The new approach usually raises cultural issues. It is difficult to implement a strategic risk management system in an organisation with a decentralised culture, because it requires a high degree of co-ordination and co-operation. Organisations with decentralised functions are often concerned with not destroying the innovative and entrepreneurial spirit of their employees.

4. Inadequate I.T. systems

Collecting information, organising it and creating a database requires I.T. systems that satisfy the needs of the risk management process. The information and the results should be automated collected and senior management should use the data to interpret and act. But several times inadequate I.T. systems have made difficult some of the above tasks; I.T. systems might require overcoming some issues regarding the compatibility of the existing systems or the transformation of the data in homogenous format.

1.4 Planning Risk Management

"The essence of risk management lies in maximising the areas we have some control over the outcome, while minimising the areas where we have absolutely no control over the outcome and the linkage between the effect and cause is hidden from us" (Bernstein, 1996).

The Combined Code by the Committee on Corporate Governance recognises that the directors as a board are responsible for relations with stakeholders, but they are also accountable to stakeholders. The directors must not run the company exclusively in the short-term interests of today's shareholders. The directors' duty is to shareholders both present and future. The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets. This covers not only financial controls but operational and compliance controls, and risk management, since there are potential threats to shareholders' investment in each of these areas. Additionally, the directors should at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. The review should cover controls, including financial, operational and compliance and risk management.

1.4.1 Internal Control – Integrated Framework

The CoSo Report (1994) by the TreadWay Commission defined internal control and it has been widely accepted as the most complete and comprehensive definition of the internal control system. This definition points out fundamental principle of a process, affected by people and providing reasonable assurance. It also includes the objectives, the components and the criteria for effectiveness. According to CoSo report:

> "Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - ❏ Effectiveness and efficiency of operations.
> - ❏ Reliability of financial reporting.
> - ❏ Compliance with applicable laws and regulations.

The first category addresses an entity's basic objectives, including performance and profitability goals and safeguarding of resources. The second relates to the preparation of reliable published financial data derived from statements. The third deals with complying with those laws and regulations to which the entity is subject.

Internal control consists of five interrelated components, derived from the way management runs a business and are integrated with the management process. The components are:

❏ **Control Environment**

The control environment sets the tone of an organisation, influencing the control consciousness of it people. It is the basis for the other components and provides discipline and structure. Control environment factors include integrity, ethical values, management's philosophy and operating style, the way management assigns authority and responsibility and others.

❏ **Risk Assessment**

A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis or relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed.

❏ **Control Activities**

Control activities are the policies and procedures that help ensure management activities are carried out and that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organisation, at all levels and in all functions and include activities as approvals, authorisations, verification, security of assets, reviews of operating performance and segregation of duties.

❏ **Information and Communication**

Information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems deal not only with internally generated data but also with external events. Effective communication also must occur in a broader sense, flowing down, a cross and up the organisation. All personnel must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

❏ **Monitoring**

Internal control systems need to be assessed through ongoing monitoring activities, separate evaluations or a

combination of the two. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures.

1.4.2 Internal Control – Guidance for Directors on The combined Code (ICAEW, 1999)

The internal control system and risk management are interrelated. The business environment changes continuously and thus the company's objectives continuously evolve. The new conditions enhance the possibility for new risk and for that reason a sound system of internal control depends on regular evaluation of risk.

The "Turnbull" report emphasises two main points:

a. The responsibility of the board of directors to maintain a sound and effective system of internal control

b. The attributes of an effective system of internal control.

"The board should consider the following factors:

- ❏ The nature and extent of the risks facing the company;
- ❏ The extent and categories of risk which it regards as acceptable for the company to bear;
- ❏ The likelihood of the risks concerned materialising;
- ❏ The company's ability to reduce the incidence and impact on the business of risks that do materialise; and
- ❏ The costs of operating in managing the related risks.

The system of internal control should:

- ❏ be embedded in the operations of the company and form part of its culture
- ❏ be capable of responding quickly to evolving risks to the business arising from factors within the company and to changes in the business environment; and
- ❏ include procedures for reporting immediately to appropriate levels of management any significant failings or weaknesses that are identified together with details of corrective action being undertaken".

These two reports endorse the importance of an internal control system and point out that an effective internal control system is essential to protect the organisation from risks. Risk management is an integrated part of the internal control system.

1.4.3 Implementation of the ERM Framework (CAS ERM-Committee, 2003; Tillinghast-Towers Perrin b/c; Chapman, 2003)

1. Establish Context

The External Context involves placing the organisation into its external environment. In this step, analysts and practitioners are trying to define the relationship of the enterprise with its stakeholders (shareholders, employees, customers, and regulatory authorities) and also the communication policies with the stakeholders. The External Context will also describe the strengths, weaknesses, opportunities and threats of the enterprise. Risk management philosophy and risk appetite have to be defined.

The Internal Context describes the strategic objectives of the organisation which are closed tied to the risk appetite and the risk management policies.

Risk Management has to identify thoroughly the risk categories that the organisation will adopt. These categories depend on the needs and the business environment of the organisation.

2. Risk Assessment

This stage will provide the necessary information to the organisation to create its risk profile. Companies whose risk profiles do not change frequently often fail to understand that risk identification is a crucial component of the risk management process. We should also point out that because risk can have positive and negative meanings the negative effect are usually addressed through the risk management process, while positive outcomes are taken into consideration in the strategy and objectives setting of the organisation. We would like also to clarify that risk is the possibility that something might prevent the achievement of business objectives, while risk factors are the events or conditions that lay the conditions for risk to be raised. For example, the damage of reputation is risk; using materials that can cause pollution to the environment is a risk factor.

2.1 Identify risk factors

This step involves gathering historical data, conducting interviews with experts from senior management, operations management and corporate staff and reviewing documents, so as to identify information on the risk factors-events that can prevent the achievement of the business objectives. This approach is adopting so as to determine the potential impact of each risk on key performance indicators (KPIs), the likelihood, the frequency and the predictability of each risk. The information have been collected will provide a valuable insight into the corporate culture, the business strategy and objectives, the control environment, as well as the capacity and the readiness for change of the organisation. It is also important to document properly all the data have been gathered. Several methods can be used, such as the risk mapping that illustrate through graphs the causes and effects of each risk, but it is considered to be time consuming and relative difficult. Another method, more simple, is to create tables where each row represents a unique risk and each column represents the information gathered for each risk.

2.2 Prioritise risk factors

Risks are rated in terms of severity, likelihood and quality of existing controls so as to determine the priority and scope. Depending on the priority of risks, these will be reviewed by the high, middle or low level of management.

2.3 Classify risk factors

One useful classification method separates risks into strategic and manageable risks. Strategic risks are usually reviewed by the board and senior management and are related to strategic decisions, like for instance mergers, acquisitions, enterprise-wide change of technological infrastructure. Strategic risks are tied to strategic decisions and may require substantial expenditures to manage them or initiation of a gradual change programme. Manageable risks are related to operational decisions. Organisation can meet manageable risks using its existing resources.

3. Risk response

This step encompasses a number of different strategies to treat risks, including decisions to avoid them altogether e.g. staying out of a particular market, reduce them e.g. though

preventative measures, transfer risk e.g. through insurance or hedging instruments or accept the risk e.g. self insurance (Outram, 1997). "Management identifies risk response options and considers their effect on event likelihood and impact, in relation to risk tolerances and cost versus benefit. Effective ERM does not mean that the best response was chosen, only that the response selected is expected to bring the risk likelihood and impact within the entity's risk appetite" (Chapman, 2003).

4. Control Activities

Control activities are the policies and procedures that ensure that the decisions were taken are followed in practice. This stage is similar to the Control environment, one of the components of the internal control system as it has been describes by the CoSo Report at the Internal Control – Integrated Framework. For that reason the control consciousness of the company plays an important role.

5. Information and Communication

Information from external and internal sources must be identified in a manner that can be transmitted effectively to everybody within the organisation, in a reasonable time frame. Significant is also that everyone in the organisation to have a clear view of his role and responsibilities so as to participate effectively in the process.

6. Monitor and Review

This step involves continuous evaluation of the risk environment and the performance of the risk management strategies. The results will show the extent to which the risks are managed by the selected strategies and will give feedback to the initial stage of the whole process. Ongoing and separate monitoring will ensure that ERM is applied at all levels and across the entity.

1.4.4 Elements of a Risk Management Culture – Investing in Success

The survey Enterprise Risk Management: Trends and Best Practices, prepared by Tillinghast-Towers Perrin and sponsored by the Institute of Internal Auditors Research Foundation identified some success factors for ERM. The efforts to implement ERM can be more successful when there is a constant support by senior management and staff is decided to make every effort towards the successful implementation of ERM. It is also important to create links between ERM objectives and the financial and strategic objectives and integrate ERM into the business planning process (Tillinghast-Towers Perrin, 2002d). Additionally, risk management is everyone's responsibility; people from IT, legal and communication departments are involved in the decision-making and inform senior management for non-financial risks that they have identified. Attention should be given to the fact the risk culture within the organisation has defined clearly. The enterprise's risk appetite is defined clearly and risk management is aligned with the business objectives and the organisations culture so as to be accepted by the staff and prevent potential conflicts (PriceWaterhouseCoopers, 2002).

COMPUTER ASSISTED AUDIT TECHNIQUES & TOOLS

2.1 Definition of CAATs

"In order to better serve the increasingly complex needs of their clients, auditors must provide a better service, while being increasingly aware of the costs. To this end, auditors are looking for computer-based tools and techniques. CAATs are defined as computer-based tools and techniques which permit auditors to increase their personal productivity as well as that of the audit function" (Coderre, 1996).

During the last decades the business environment has been changing constantly and rapidly. Technology has been one of the driving forces of that change, but at the same time it has been part of the impact of that change. The new age forces auditors to reassess their approach to auditing. Information has become strategic resource of the organisation and issues such as: who owns the information, how accurate, complete and on time it is and how well is managed concern management. If information is used effectively, then it can contribute to the organisational success.

Auditors are using data and information to analyse and assess the current state of the business and then to recommend on the internal control system and thus on the business objectives and the potential success. Given that organisations are adopting a client-satisfaction approach, if auditors want to add value they might consider involving technology at their work and transforming manual audit tasks to automated audit, whenever this is applicable. Moreover the volume of data has increased dramatically and has become more complex than it used to be, so the need for quick and reliable methods of information location has become an opportunity for further development.

"Many experts have observed that the change of information technology is longer linear. Increments of value produced by new technology arise from very different technologies, and not by the old ways of improving processing speed, increasing storage, or reducing unit costs. This means that even small but enterprising businesses can create value and also those companies are concentrated on what the new technology can do rather how it can be controlled" (Raval, 1998).

Some audit organisations believe that audit software is costly and cannot be proven cost effective. Audit software may run only on mainframe computers, may require site licences and expensive maintenance contracts or need significant amounts of programming. Most of the time audit packages have to be developed and programmed by a programmer. If the programmer does not have any audit expertise, then he might develop software that does not meet the requirements of the audit activity or he might develop an interface that it is not friendly to the user. Additionally, training requirements are expensive and it therefore can be difficult for a company to use them. The shift from manual audit to automated activities might enhance the belief that the possibility for corrupting or deleting data is increased. Some CAATs are so general that customising them for specific use might be a complex process. However, the current audit software offers more choices and the costs have decreased dramatically. Modern audit software is more flexible and can be used to analyse data from a variety of applications on various computer platforms. Beside, software vendors have developed audit packages that can be used easily by auditors (Coderre, 1996).

2.2 Classification of Computer-Assisted Audit Tools And Techniques

Computer-assisted Audit Tools and Techniques can be classified in the following groups (Le Grand, 2001):

1. Electronic WorkPapers
2. Information Retrieval and Analysis
3. Fraud Detection
4. Network Security
5. Electronic Commerce and Internet Security
6. Continuous Monitoring

1. Automated WorkPapers (Chapman, 2002)

Automated WorkPapers facilitate communication within the internal audit department and between the auditors and the clients, due to their standardised format. Auditors know what areas and data they have to cover and by that way they communicate more effectively among them and with the clients. Michael Tush, director of IS Audit and John Daniels, IS Auditor in the Wal-Mart Stores are using TeamMAte, an electronic workpaper to perform their audit work. They also use it in the planning phase to set the objectives and the scope of the audit program. An automated work paper, like TeamMate is also used to provide data for a library of audit information. This library contains information for previous and current audit and so it can be used as a database feedback and guidelines for future audits. Attention should be given to the environment in which the software will operate and also its available flexibility.

2. Data Extraction and Analysis

The software tools that have been developed for information retrieval and analysis purposes give the opportunity to auditors to access all the stored data. The data may be stored in various formats and in various operating systems, but with appropriate and experienced operation can be extracted and analysed (Le Grand, 2001). The audit tools convert themselves the data into the appropriate form. This helps to maintain independence, and avoid corruption during conversion. Some of the most popular software for data extraction and analysis are the ACL-Automated Command Language and the IDEA developed by the Canadian Institute of Chartered Accountants (CiCa) and Excel by Microsoft. The respondents from the survey on the most popular audit tools that was conducted by the IIA's global information network (GAIN) provided us with statistical information on the usage of the audit software (McCollum et al., 2003) The data showed that Excel is used by a lot of auditors to retrieve and analyse information. Harold Lederman, Chief Internal Auditor of the Saint Vincents Catholic Medical Canters of New York uses Excel for data analysis. He seems to be enthusiastic and praised Excel for its efficiency, multiple statistical calculations and ability to help effectively on various audit activities. Although, we appreciate the capabilities of this particular software, it is worth mentioning that Excel can be useful for several basic audit tasks, but it can be good as long as the amount of data does not exceed the limits set by the software. Excel has approximately 66,000 rows of data, something that makes it incapable to work on large files. In addition, as Mr. D. Price said "I consider this as dangerous, because Excel is good for what it does, but many people do not understand the controls that need to be around, because if we are using it to analyse data, we have a limit of 67,000 records, so we cannot use large files. There is no audit trail, so we do not know what we have done, there is any change control management and so we do not know who is changing the formula and we do not have any data integrity. The last happens because we do not know if any of the cells has been changed. If we want to manipulate data during the analysis, then it is easy to be done, while when using ACL or IDEA they are read-only products and so they have restricted access on the source of data" (Price, 2003).

3. Fraud Detection

Accounts payable, employee payroll, expenses reporting and inventory management present the most high-risk areas for fraud incidents. The usage of audit tools, like the ACL and the IDEA has been proven helpful during the procedure of identifying fraud indication. Amongst their various capabilities they are also included the location of duplicate payments, unusually high credit payments, data that do not need much certain and logical requirements, like for example duplicate post code or telephone number or invalid format (e.g. telephone number that applies to two different suppliers or with invalid format). In an advanced level, the software may have databases with key features of fraudulent indicators that are using during the tests to find similar entries in the system (IDM, 2003).

4. Network Security and Performance

Companies' dependence on information systems has lead to the increase of the fear of unauthorised intrusion on their local Intranet, which in turn has increased the demand for Internet security. Section 404: Management Assessment Of Internal Controls of the Sarbanes-Oxley Act requires "each annual report of an issuer to contain an "internal control report", which shall:

i. State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
ii. Contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting" (AICPA, 2002).

The issue of the Sarbanes-Oxley Act has forced a lot of companies to comply with these requirements. Nowadays, more and more companies depend on information technology systems for the preparation and issue of their financial statements. Software programs like the BindView, developed form the BindView Corporation promises that "helps organisations to automate the development and distribution of their security policies, then easily deploy them across the enterprise. Tailored policies can manage and control activities ranging from assessing business continuity procedures to deploying or patching servers and workstations" (**http://www.bindview.com**). "The Internet Scanner application, another software developed by Internet Security Systems' (ISS) provides automated network vulnerability assessment across servers, desktops, and infrastructure devices. Internet Scanner performs distributed or event-driven probes of network services, operating systems, routers/switches, servers, firewalls, and application routers to identify potential risks" (**http://iss.net**).

Despite the capabilities of the various software to provide assurance and security on the network security and performance, it is important that auditors during their assessment and evaluation on the internal control system not to disrupt the normal operation and performance of the network.

5. Electronic Commerce and Internet Security

The increase of electronic commerce and the exchange of information via the Internet drive the need for safety. The auditors' role lies on the responsibility to provide assurance of

the security of information and systems that send or receive data through Internet connection. Firewall software or intrusion software is used to reinforce the safety of the information systems.

6. Continuous Monitoring

Integrity and accuracy of the published financial information and immediate access to information by the organisation's staff and stakeholders require direct response form auditors. ACL, IDEA, Excel or internally developed software are some of the tools used for continuous monitoring purposes.

2.3 Benefits from the Use of Computer-Assisted Audit Tools & Techniques

The use of information technology in audit offers numerous benefits (Coderre, 1996):

- ❑. "improved efficiency, effectiveness through planning, conduct and reporting phases of the audit
- ❑. ability to evaluate a larger universe and increase audit coverage
- ❑. increased analytical capabilities
- ❑. improved quality of activities performed during the audit
- ❑. consistent application of audit procedures and techniques
- ❑. increased cost-effectiveness through the reusability and extensibility of computerised techniques
- ❑. improved integration of financial/information systems audit skills
- ❑. increased independence from information systems functions and greater credibility for the (audit) organisation
- ❑. greater opportunities to develop new approaches"

The benefits of CAATs can be obvious at all stages of audit process. In the planning phase, audit software can help management to select the audit areas, identify initial risks and determine preliminary objectives. CAATs are used extensively during the conduct phase. Finding from the tests that were performed with CAATs, may call for further investigation and give auditors the opportunity to apply critical thinking and reasoning, rather than only compliance with fixed rules and controls. CAATs can be used to select statistical samples or to improve the effectiveness of a judgmental or direct sample. They can also provide to the organisations the ability to conduct audit in areas that was not previously possible due to the large number of transactions and tests that should be performed. Use of technology allows auditors to spend more time on activities that require the auditor's judgement.

The use of CAATs can benefit any audit department, regardless of its size or current technology. The level of CAATs varies among organisations but it is not necessary to develop complex audit routines, because simple use of the computer can achieve quick and reliable results.

Audit software has been popular during the last decades due to the fact that the software applications audit through the computer, rather than around the computer. This option creates the ability to extract and examine accounting data in a time frame much shorter than before and also conduct 100% testing. Auditors develop a better understanding of the business, because they are able to examine a larger volume of data and in that way they get a broader view of the enterprise. Another implication is that they can reach more precise conclusions, because they view and analyse all the data and files, instead of trying to extrapolate information from a limited volume of data. (Lanza, 1998) Except from the benefits of the computer audit tools, potential disadvantages exist when they are used. Dependence on technology to perform audit tasks can put in danger the thinking process of the auditors, because prior manual audit tasks are now performed automatically. In addition, increase of audit coverage results to more information and evidence on the quality and performance of the internal control system. This new information may require further investigation, but this raises the problem of available resources, in terms of funds, time and staff. So instead of benefit the organisation, the audit tool may complicate things more and involve the organisation to a non-ending investigation even of the smaller and less significant function within it.

Audit software has been used in practice and it has proved that it can increase productivity and can give the opportunity to auditors to gain time by automating manual audit tasks, so as to devote more time to other activities. Use of audit software represents the forward-looking and future-oriented approach of auditors to their profession. Effective use of computer technology by exploiting all the potential capabilities meet the expectations of the clients for high quality of services, sufficient return on investment on technology, provide audit staff with the most productive tools and offer value-added services.

2.4 Developing CAATs Capabilities

Computer-based tools and techniques can be proved very useful in terms of time and cost savings, but in order to work efficient and effectively, a plan for their implementation should be done. Coderre (1996) and Paukowits (1998) offer describe the steps of that plan.

❑ **The new future – resistance to change**

Change is a vital and integral part of organisational and social life. Introducing computer technology in the audit department, which was working with traditional methods-manual audit instead of automated audit, is perceived within the context of change. Introducing new technology in an environment that did not use it in its operational activities is considered as one of the typical cases of organisational change. This last thing is that makes change and consequently the usage of CAATs such a controversial matter and an issue of conflict is that usually faces resistance from staff, line management and senior management. People within the audit department may perceive CAATs as a threat to the previously safe and stable conditions; new ideas and new methods imply also change of the organisational culture of "how things used to be done until that time". Considering all these, it is obvious that management has to understand the nature, the reasons for and the implications of the resistance to change and develop a clearly defined strategy of managing change (Mullins, 2002). Ideally, management has to promote CAATs as an opportunity for innovation, creativity and forward thinking.

❑ **A champion to lead**

At the early stages of the implementation it would be useful if the project team were able to identify a person who will be responsible to transmit the benefits and the potential success of the implementation, someone who will mobilise interest and provide support. In order to maintain interest in CAATs stories

of successful events should be reported to staff. The champion should have sound, visible and vigorous appearance within the organisation and provide feedback to management.

❑ **Organise a training program**

The purpose of this stage is to involve top-management and also provide high-technical training to the staff that will use CAATS. Time should be spent so as to develop a training program that meets the needs of the organisation in terms of personnel skills, level of difficulty using the software; pace of improvement of the audit activity and the emergence for quick improved results. Careful selection of the staff members that will participate in the training program is essentially so as to ensure that only staff with adequate audit and computing skills is trained. Senior management should participate so as to become familiar with the capabilities of software and enhance the possibility for acceptance without significant resistance.

❑ **Management commitment**

Senior audit management has a primary responsibility to set the tone at the top and create the conditions for successful of CAATs. Gaining commitment from the entity's management is a key factor for successful implementation of CAATs. After the training program, senior management has become familiar with the capabilities and the potential benefits of CAATs, whereas the champion has also introduced and effectively communicated success stories to management.

❑ **Set targets**

Introducing a new technology in an organisation should be accompanied by well-defined objectives, that they meet the expectations of management and fully explained why this new technology is necessary. They should not be very optimistic, but just realistic. There are several factors that should be taken into account when we set the targets, for instance:

- ❑ Evaluate the required resources (staff, hardware, software, etc.)
- ❑ Give priority to the most important tasks.
- ❑ Plan a time schedule.
- ❑ Produce a cost benefit analysis.

❑ **Giving evidence – conduct a pilot**

Given that the project team has planned it carefully, performing a pilot of the specific application will allow management to devote resources on the new technology. Testing the software will give evidence on the savings on time and resources and will convince on its quality. A successful pilot means that proper planning should be done, so as to create an environment where testing will reveal the real benefits of the new application. Choosing the right people, who have the right skills and knowledge; the right audit, the manual audit should be ideal for transforming it to automate like for example sorting, matching, analysing data and also the right time, the right tools and techniques will create the conditions for success. A final report should include a cost/benefit analysis, which should highlight the benefits of the audit software to the audit department and to the organisation in terms of cost savings, efficiency, effectiveness, quality of results and other key attributes. The final report should focus on the fact that the new application will provide improved performance to other audits also.

❑ **Provide assistance**

If the organisation has centralised IT support, then organising working groups, which will support the application of the computer software, can do the transition to a more proactive and practical approach and the auditing department will facilitate the implementation of CAATs. Two working groups are usually enough to provide adequate support. The first working group will be responsible to introducing computer terminology, teaching and explaining basic concepts and functions like sorting, matching, extraction etc. Examples of real audit tasks will assist in making auditors feel comfortable with the new technology and appreciate the capabilities of the application. The second working group should be more expert on CAATs applications and should be committed to educating auditors on the organisation's information systems. This working group has to set priorities on which information system will be examined and tested, for example finance or human resources or logistics department, and has also to decide on the structure of the team. Ideally it should consist of a team leader and members who are experts on information systems, auditors and specialists on the specific information system. Usage of specialists should draw the attention of the team. They can provide their advice on the various issues of the implementation, but it has to be ensured that auditors always control the functions and commands of the application and that management does not interfere with the assessment of the internal control system. At the end of the training sessions, a report with the results should be distributed to all the members of the audit department. Issue of a manual handbook would be helpful and would encourage individual effort and initiative.

At this stage of the process it is important to share the results of the efforts with the employees and inform them about every success or failure. By that way participation consciousness is increased and employees start to consider the new application as an integral part of their work. Ongoing monitoring of every activity is essential to evaluate the performance and effectiveness of the software as well as of the employees. Monitoring daily practice will give information, which eventually will improve performance and successful implementation.

❑ **IT support**

Common practice suggests that IT support should be provided preferably by in-house developed employees rather than from outside consultants. The second choice should preferably be avoided because it might imperil the accuracy of the audit results and thus the efficiency and effectiveness of the audit department, e.g. issue of independence may arise. Usually, organisations are facing the dilemma whether to develop audit skills on the IS experts of the organisation or to develop IS skills on the auditors of the organisation. The basic problem with the first choice is that IS experts due to their lack of audit experience may not recognise potential audit areas where CAATs can be used. Whatever the choice is the final outcome should be directed to have one or two individuals who will combine IS skills and audit experience. In that way, we ensure that the combination of both IS and audit skills will allow the performance of their tasks based on an auditor's perspective and on an IS's expert view.

2.5 Continuous Auditing

Continuous auditing is defined as a comprehensive electronic audit process that enables auditors to provide some degree of assurance on continuous information simultaneously with, or shortly after, the disclosure of the information (Rezaee, 2002). Continuous auditing is not a recent phenomenon. Even 3 decades ago, continuous auditing had been a way of protection against fraud and malpractice, but it has recently come to the fore due to the enormous scandals of Enron and WorldCom.

Auditors and accountants are searching for the best practices in order to prevent irregularities. There are also other factors that reinforce the necessity of continuous auditing, such as the highly sophisticated systems used by the organisations, the greater volume of data processed by these systems, the online publication of financial information and the "enhanced responsibility of management for the adequacy of internal controls" (Shields, 1998).

It is worth mentioning that a debate over the accuracy of the statement *continuous auditing* has been raised. Dr. John Mitchell, managing director of LHS Control, believes that continuous auditing is a wrong statement. Assuming that it is management's responsibility to control the process, then management needs continuous ***monitoring*** to show that the process is being well controlled. The audit is a check that continuous monitoring is working (Mitchell, 2003). It is believed that there is red line between continuous auditing and continuous monitoring, crossing that line by auditors means that their independence will be jeopardised.

Continuous auditing through the computer highlights a change for the audit profession. Auditors have to expand their activities on the risk profile of the organisation by evaluating the internal control system, and make recommendations on controls. They also have to develop a thorough understanding of the business objectives and the business strategy and use modern computer techniques such as audit embedded modules and automated software that meet the needs of the audit engagement (Rezaee, 2002). CAATs can be used for various reasons and can have multiple uses. Given that some of the controls are programmed through the computer and data are stored in the computer, then CAATs can be used, to test the security level and also for data extraction, sorting, matching and to identify duplicate records, e.g. in the payroll system. These results are used to evaluate, as far this possible, the internal control system and to identify risky areas, e.g. suppliers. Savings in time, cost and effort enhance their use. Using CAATs in continuous auditing confirms the essence and definition of continuous auditing, a natural development of the traditional auditing to a modern approach that provides greater assurance, credibility and accuracy.

Continuous auditing has the advantage that it audits the transactions at the time they occurred: continuous auditing is a real-time system. Continuous auditing can be described as the ultimate and most effective form of preventive control. Moreover, continuous auditing provides assurance about the information used for the decision-making process (Rezaee, 2002). Update information for the integrity of the published information, the efficiency of the operational controls could be used to create a balance scorecard database within the organisation for non-financial characteristics. Continuous auditing is a prominent principle because all the information is relevant to decision making. Information from the finance department is related to the financial performance of the organisation, information from the human resources department will be used to measure the performance and productivity of the employees, information from the logistics department will show whether or not the company keeps inventory for a long time and misses the opportunity to invest this money on other more profitable sources. The information from each different department is related to each other, because if we combine them all together will give us ways to improve the performance of the entity in a total manner. Organisations are looking for solutions to gain competitive advantage in the market in which they operate. Information has to be reliable, accurate and being provided on a regular and timely basis.

Continuous auditing through the computer has to fulfil some essential requirements in order to be successful. "Effective development of continuous auditing methodology requires creating an information technology infrastructure for assessing and retrieving data with diverse files types and record formats from different systems and platforms" (Rezaee, 2002). This last statement should not be necessarily interpreted as integration of systems and sub-systems. Depending on the organisation's needs and on the features of the audit tool, integration of all the systems may not be beneficial. The problem that appears with the software that is integrated to the organisation information system is that it is controlled with difficulty; large applications like SAP cannot be handled easily and another problem is that if there is a flaw or defect on one part of the system, then the whole system will be affected. The degree of automation varies with the design of the audit system and also the implementation plan. The different level of implementation impacts also on the involvement or non-involvement of the auditor in the process. Highly automated auditing includes embedded audit modules and highly integrated systems; on the other hand less automated auditing will still enable loading and processing of data, but will require the involvement of the auditor. In addition, auditors should have the necessary qualifications to undertake such an audit engagement. Knowledge of the subject that is audited and also about information technology issues is essential; recruitment of external consultants is a frequent solution. Each software is good as it has been designed properly and each software is effective, as it is been used efficiently by exploiting effectively.

THE ROLE OF THE INTERNAL AUDITOR IN RISK MANAGEMENT

3.1 Role of internal auditor in risk management

The new set of Standards for the professional practice of Internal Auditing (1999) boost internal auditing function to a higher level and induce internal auditing to become an active member of the strategic process of an organisation. Until the rewritten Standards, the traditional role for internal auditor was to provide assurance to management, but with the new Standards internal auditors are challenged to participate in the governance and risk management system of an entity. Assurance is related to history and to past events, while risk management and governance are related to the present and the future of an organisation. Risk is linked to strategy, because it represents the obstacles to the achievement of the objectives and the goals of an organisation that are necessary for an organisation to continue to operate and increase its value. If internal auditors are involved in risk management, they are getting closer to strategy and interact and cooperate with senior management.

Each organisation establishes its strategy and its objectives. These are based to the future plans of the organisation, the available resources, the information derived form a market analysis, which shows the existing and potential competitors and their activities and the available market opportunities. Whether or not risk management is formal and continuous procedure within the organisation, everybody accepts the fact there are impairments towards the implementation of the business strategy and the achievement of the objectives. These impairments are represented as risks, since risk is recognised as a situation or factor that has material effects on the business operations and performance. The responsibility to identify those

risks and decide which strategy should follow in order to manage those risks lies with senior management. The primary responsibility lies with senior management, but everybody in the organisation has also responsibility, as far as its position, capabilities and duties permit to have. So, management establishes several measures and controls in order to protect itself form those risks, for example it will use an intrusion detective software to protect its information systems for unauthorised intrusion or it will prepare a contingency plan to enable the information systems to recover and rebuild its operations (Weber, 1999) or will hedge its position by using financial instruments like derivatives, mutual funds and governmental bonds.

Standard 2110 for the Professional Practice of Internal Auditing (1999) suggest that:

2110-Risk Management

The internal audit activity should assist the organisation by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.

***2110.A1**- The internal audit activity should monitor and evaluate the effectiveness of the organisation's risk management system.*

***2110.A2**-The internal audit activity should evaluate risk exposures relating to the organisation's governance, operations, and information systems regarding the:*

- *Reliability and integrity of financial and operational information.*
- *Effectiveness and efficiency of operations.*
- *Safeguarding of assets.*
- *Compliance with laws, regulation and contracts.*

Internal auditors will review and evaluate the internal control system of an organisation and will decide whether or not it protects the organisation from the various risks. In the case where the internal control system works properly, indicating that controls are adequate to meet effectively the business risks, internal auditor may or may not have recommendation for improvement, depending on his or her experience and knowledge. In the case where the internal control system does not work properly, then the problem might be that the established controls do not confront efficiently either the risks that have already identified by the organisation or new risks have appeared, but the existing controls are not adequate to prevent any material loss to the organisation. At the last two cases, internal auditor has to recommend more effective controls. The approach that has already been described is simplistic and is closer to the traditional role and approach that an internal auditor takes against any procedure or system of an organisation. The following diagram presents a more complex and systematic outline of the role and function of the internal audit department in the risk management process (McNamee & selim, 1998)

A MODEL FOR IMPROVING INTERNAL AUDIT SERVICE TO THE ORGANISATION THROUGH RISK MANAGEMENT TECHNIQUES

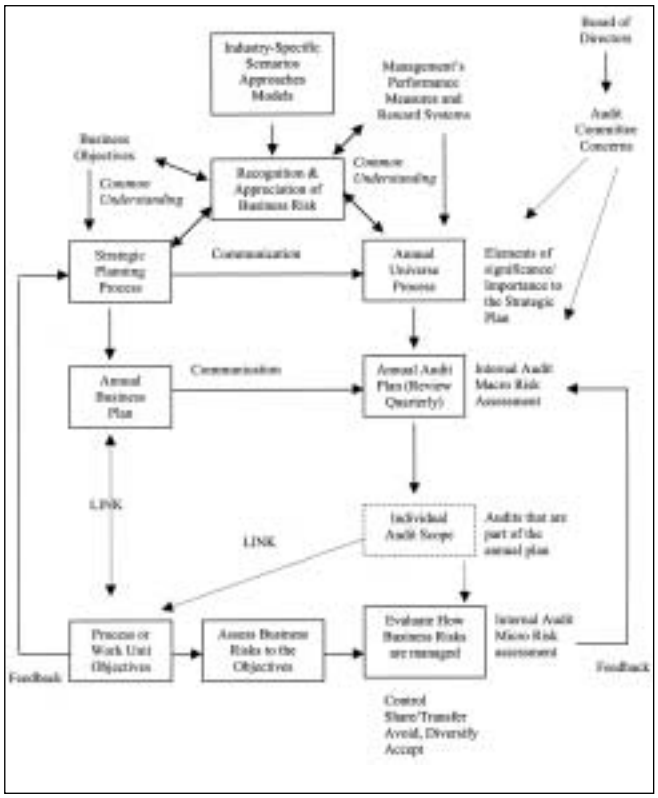


Figure 2: The Validated Descriptive Model of Integrated Risk Management and Internal Auditing

Source: McNamee, D. & Selim, G. M (1998) Risk Management: Changing the Internal Auditor's Paradigm, The Institute of Internal Auditors, Research Foundation, USA

McNamee and Selim (1998) have used the diagram in figure 2 to describe in a very effective and explicit way what has already described. The validated model describes how the internal audit department can contribute in risk management, by incorporating its activities smoothly and gradually to the strategic and operational activities of an organisation. The organisation sets it objectives, recognises and appreciates the business risks. It develops risk models and scenarios so as to gather information and to develop its strategy. The important element of this figure is the connection between the strategic process and the audit universe process and also between the annual business plan and the annual audit plan. Additionally, the direction and the content of the communication between senior and operating management and internal audit department is also a fundamental prerequisite of the success in the integration of risk management and internal auditing.

Senior management establishes its strategic process that suits best to the fulfilment of the business objectives. "The audit universe is the sum of all the auditable units for an organisation, where auditable unit is any particular topic, subject, project, department, process or function that is worthy of an audit" (McNamee & Selim, Glossary, 1998). The internal audit team has to set the criteria to decide what are the most important elements to be audited. The strategic plan includes the

strategic objectives of the entity's. Given that internal audit has as purpose to provide assurance to management, when it is aware of the business objectives, concerns and decisions of the organisation, it can incorporate all these information to define the audit universe. By that way internal audit has a clear picture regarding the direction of its activities, it adds value to the organisation and convinces management for the real value of the internal audit function. This last is really important since internal audit function is considered by some organisations as an additional burden. Dr. John Mitchell (2003) suggests that many organisations have internal audit department only due to compliance to laws and regulations and not because they recognise the benefits form the internal audit. He also suggested that 40% of the FTSE 100 companies do not have an internal audit department because they think that it does not credit for its merit. Whether we consider this statement as an entire or partial truth, internal audit has an additional motive to involve in a process such as risk management, so as to persuade for its value. By communicating the business strategy to internal audit and defining the audit universe by including all the important elements of the strategic plan, we avoid to perform audit after the results have been appeared and internal audit function find its role at the beginning, there where everything starts. If the audit universe contains elements of the business strategy, then internal audit is working parallel with senior management and it is aware of its concerns and the business risks. So, internal audit department drives its activities, except from the traditional compliance audits and operational reviews, to a strategic level and to a risk-based approach. Nothing from all these imply that internal audit should involve in and control the strategic planning process.

At the operational level, management develops its annual business plan according to the requirements of the strategic plan and also the risks, both inherent and form the external environment identified by management so as to demonstrate proactiveness rather than reactiveness. In the same way, internal audit can develop the annual audit plan by taking account the objectives and the high-risk areas identified by management. Frequent reviews of the annual business plan and the audit plan are essential so to keep them updated and informed of any external or internal changes.

Internal audit will capture all the information derived from the strategic process and the business plan, for example the objectives of the organisation and how management plans to achieve those objectives, form the risk assessment, i.e. the identification, measurement and prioritisation and also the activities and controls set by the organisation to manage those risks. Internal Auditors' job begins by monitoring these activities, perform tests for the effectiveness of the controls and evaluate of how the business risks are managed. At the end of each audit engagement, auditors have to submit an audit report describing the procedures that they followed, the tests they performed and the major findings and recommendations.

The Position Statement on the role of the internal audit in risk management by the Institute of Internal Auditors- UK and Ireland (2002) gives some guidance on the role of the internal auditor in risk management and makes clear that "the role of internal audit within risk management cannot, and should not, be prescribed. The role within one organisation may change over time and the role from one organisation to another is likely to be very different. Each internal auditor must determine the most appropriate role for their organisation and supply the required services. When determining the most appropriate role to play, internal auditors should pay heed to the professional requirements for independence and objectivity and should ensure that these are not breached. They also must be certain that they have the necessary knowledge and skills to play the role they adopt within the risk management process".

The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC), and ALARM The National Forum for Risk Management in the Public Sector has recently published the new Risk Management Standard and adopted the proposed role of the internal auditor by the IIA UK and Ireland (2002). In this position statement, internal auditor is advised to focus the internal audit work on significant risks, identified by management, auditing the risk management process and provide assurance on the management of risk. If internal auditors want to communicate effectively with senior management, then they have to gain its support for the internal auditing's risk-based approach and objectives. Internal auditors can gain support, by describing the audit process for risk management that agrees with the needs of the organisation. Internal auditors should be aware of the concerns of management and the audit process should embrace management's view on risks and priorities for an effective risk management plan. Also, a common set of definition of terms used in risk management will provide the base for mutual understanding. Auditors can contribute their experience and knowledge on control and risk analysis on the development of the strategic process, while on the same time they ensure that the annual audit plan will reflect the priorities of management on the high risk areas (Leithhead, 2000). He can also take a more active role and provide support and participate in oversight committees and monitor activities and reporting procedures. Furthermore, internal auditor can act as facilitator on risk assessment workshops and co-ordinating risk reporting to board, audit committee and risk committee by establishing formal procedures of reporting. Report to management should be a comprehensive description of the risk model, the risk factors, the impact, the techniques of managing those risks and how the potential risk arising from any department interact with the others and affects the business performance of the whole organisation.

3.2 Use of Computer Assisted Audit Tools and Techniques in Risk Management

CAATs mean computer assisted audit tools and techniques and are used primarily to analyse data on a computer system. We can use them within risk management process to verify that the controls are working. So, CAATs are an assurance provider. Management is responsible to manage risk, if they say that a risk at the inherent level is 5.5 (*inherent risk is the risk found in the environment and in human activities that is part of existence*, Glossary by McNamee & Selim, 1998) and at the residual level is 1.1 (*residual risk is the risk after risk management techniques have been applied,* Glossary McNamee & Selim, 1998), they have to proof that these controls are working. If the controls are on a computer system, we can use CAATs if the controls are working (Mitchell, 2003). So, we can use CAATs mainly when we have to deal with quantitative information and we want to transform them in qualitative information. Dick Price, an expert on computer assisted audit techniques, shares the same opinion with Dr. Mitchell and added that usage of CAATs is possible only when we deal with quantitative data and activities that have happened, by interpreting what is going on and we have to be creative when using them.

Audit software has limited use in risk management, especially at the strategic level. We cannot use it to collect information

about the competitors or to decide whether to enter or not to a new market, but we can use audit software on tasks where numerical data or data with specific format recognised by the software are available. At the top of the risk management process, we place the strategic risks and at the bottom the operational risks. Risk management is a top to down and a down to top process. The connection between operational and strategic risks is the information. Having accurate and adequate amount of information, we can reduce the strategic risks. Having managed the strategic risks, we can spend time oh identifying risk areas on the operational functions of an organisation. If we protect the company's operations, for example the assets, ensure that the payroll system works properly, e.g. no duplicate payments are occurred, the information system is well organised and maintain the acceptable level of security, then we preserve the core functions of an organisation. We cannot proceed to strategic actions, if we have not already ensure that the operational departments, like the Finance, the Inventory or the Information Technology department have identified, assessed and prioritise the risks tied directly to their operation. Everything starts from the basic concept that risk of an individual department is also a risk of the whole organisation. Based on that concept, Enterprise Risk Management finds its principles and application. Strategic risk management and operational risk management constitute decision-making process, which in order to be effective need the right information and analysed by suitable people. Well-educated and experienced staff, modern I.T. facilities, support and commitment from senior management enhance the possibility of success. Since information is a key aspect of risk management, we should anything to fulfil that requirement.

Internal audit department and audit software tools have a key role within this context. If the internal auditing has gathered appropriate information, then it can improve its role in risk management, because the information will give to internal audit the essentials to be prepared in advance and take better decisions. So, information is considered as a fundamental prerequisite for good decision making and thus for effective risk management and internal audit. Savings in terms of money and time has always been an objective of organisations, and for that reason IT facilities and technology advances have been used to enhance the progress, the effectiveness and the efficiency of the operations. The vital assistance of audit tools in risk management and generally in the decision making process is that they can provide large amount of information quickly.

Increased pressure from statutory regulatory authorities and other professional bodies for improvement of governance and risk management systems has forced many organisations to devote time and funds to build a risk management environment within the organisation. This attempt is complemented by usage of software for risk management purposes. Auditor Leverage, AutoAudit, TeamMate, Excel and internally developed software are used for risk assessment and analysis. Organisations also use ACL and IDEA, amongst other software, to monitor high-risk transactions, to track and produce exception reports (McCollum & Salierno, 2003).

ADM PLUS 1.4 for Windows is a software package, which includes risk assessment as an integrated part to its audit management function. It can be used by all type of organisations and audit department and due to its flexibility and adaptability it fits in any structure. It is ideal for multinational companies with many divisions or subsidiaries to many countries, because it can be configured to multiple to business units, each with a separate risk model. The user must perform the risk analysis, but the software can perform trend analysis and "what-if" analysis (Glover et al., 1999; http:// www.pleier.com).

Audit Masterplan 6.5 has developed by J.E. Boritz Consultants Limited, a privately owned company and supported by the Institute of Internal Auditors. The vendor describes Audit Masterplan as a scientifically designed computer-based risk assessment, planning and work system for internal auditors. Risk assessment is one of the modules included in the software, there are also audit universe management, short and long term planning, personnel skills management, recommendation manager, time reporting and activity monitoring. Amongst its advantages are that the risk model can have up to 40 objective and subjective risk factors. It can also gather evidence and data from various sources and produce a risk assessment, by giving the total control over the model (http://www.jebcl.com).

Audit software is effective in that it captures and presents information in a format easily understood by management and assists the internal audit process. There are three critical features that must be combined in software (Anonymous, 2001; Teiheira, 2001). The first is related to the usability of the software package, which preferably should not require extensive training, over-specialise skills to operate it and significant amount of time to reach to the final results. Data accessibility is also essential and related to the ability of the software to search across the entity's information systems, collect data and, present them in a meaningful format and bring together all types of risks from the business. The software must be able to meet the long-term needs of the organisation. If it is used extensively and undertakes large tasks, then it has to be ensured that it can offer friendly to user services, without complex procedures, easily understood by everyone and produce meaningful results. The IT and audit department have to prepare and plan the upgrade of the software and have made tests before the final usage. In addition to all these, well-organised reporting systems and build of a proactive character of the tool will enable the success of the implementation.

CONCLUSION

The results from the survey from CFO Research Services (2002) and information from personal communication (Mitchell, 2003) has shown that until now senior management has not paid too much attention to developing an organised and productive risk management process and they have to devote time and resources, if they want to claim an effective risk management system in their organisations. Risk management has to be an ongoing process, because we cannot manage risks effectively, if we do not constantly revise the risk assessment and mitigation techniques frequently. Risks depend on the external and internal environment of the organisation, which both of them are changing continuously. Successful risk management means immediate response to the threats and for that reason the risk profile of the organisation has to be updated regularly. Since information is so important to manage risks successfully, organisations have to find solutions to produce the desired results. At this point, Enterprise Risk Management offers a unique opportunity. The emphasis on Enterprise Risk Management is founded on the fact it provides a holistic and forward-looking approach by identifying the risks across the organisation. The basic concept of ERM is that we cannot discuss about effective risk management of risks, if we override a fundamental principle of life, which says that we cannot consider our lives independent from the pilgrimage of the rest of the world. If we put an organisation in the place of each individual life and the economic, business, technological, social, environmental and legal environment in the place of the whole

world, then we can easily accept that all these affect the performance of each organisation. But an organisation also creates its own environment through its staff, technological infrastructure, resources, plans and objectives. Risks are arising from both types of environment. What is important in Enterprise Risk Management is that recognises the fact that each small part of the organisation (i.e. department or division) interrelates with the other and all together build the risk profile of the company.

Internal auditors can contribute to the risk management process, if they change their focus from control-based to risk-based approach. The internal control system is something more than simple compliance with laws and financial reporting regulations, it ensures the continuous operation of an organisation by protecting it from various risks. A proactive approach suggests that we act in advance and this where risk management finds its role. Depending on the needs of each organisation, internal auditors should prepare and review the internal control system not only to identify whether it operates according to prescribed procedures, but also whether it protects the organisation from it current and future risks. They can also undertake to prepare the technological infrastructure to implement Enterprise Risk Management, like for example ensure that the organisational information systems are secured and that they are able to provide fast and reliable exchange and source of information. Audit software can be used to create databases of information, where the software can perform risk assessment analysis. Other software can be used to identify risk areas. The Internal auditor should have business expertise, so as to be able to understand any business procedures, decisions and systems. But the organisation has to give the internal auditor the opportunity to be involved in key decisions for the organisation, such as mergers and acquisitions. Internal auditors can also provide training to employees and transmit overall and individual responsibility within the organisation. The Chief Internal Auditor can play a significant role of the "ambassador" of the ERM policies and concept.

Enterprise Risk Management can benefit the internal audit department. Implementation of risk management with enterprise-wide focus will lead to greater amount of information, more complete risk profile and thus better risk analysis. The results can be used by internal auditors during the audit planning and on their recommendations and achieve efficiency, effectiveness and economy of resources. They are going to be able to provide more innovative solutions and become an integral part of the organisation and gain the respect and the recognition of their value (Walker et al., 2003).

Some argue that if internal auditors are involved in the risk management process, their independence and objectivity will be jeopardised. To those who support this argument, we point out that the process itself can be without flows and the critical issue might be how the procedures and plan are implemented. Another issue of criticism could be that the companies that do not have risk management procedures do not show adequate responsibility towards their shareholders and stakeholders. Both of these issues can be attributed to bad corporate governance. In order to implement risk management and also to have internal auditors in this process, we need strong representatives of corporate governance like for example audit committee, risk committee and non-executive directors who will ensure that the board and senior management act for the benefits of the shareholders.

REFERENCES

1. Anonymous, *Avoiding Bloatware,* **Internal Auditing & Business Risk,** June 2001.
2. Banister, J. (1997) *How to manage Risk*, 2nd edition, LLP Ltd, London.
3. Bernstein, P. L. (1996) *Against the Gods – The Remarkable Story of Risk*, John Wiley & Sons, Inc.
4. Casualty Actuarial Society, Enterprise Risk Management Committee, *Overview of the Enterprise Risk Management*, May 2003.
5. CFO Research Services, (2002) *Strategic Risk Management – New Disciplines, New Opportunities*, March 2002, http://www.aon.com/publications
6. CHAMBERS, A. (2002) *Tolley's Corporate Governance Handbook*, The Cromwell Press Limited, UK. (B)
7. Chambers, A., Selim, G. & Vinten, G. (1987) *Internal Auditing*, 2nd edition, Pitman Publishing, U.K (A)
8. Chapman, C. 2002 *Audit Software Usage Survey*, **Journal of Internal Auditor**, August 2002, Vol. 59, Issue 4, p128.
9. Chapman, C. *Bringing ERM into focus*, **Journal of Internal Auditor**, June 2003, Vol. 60, Issue 4, p9.
10. Coderre, G. D. (1996) *CAATTs and other Beasts for Auditors*, Global Audit Publications, Canada.
11. Committee of Sponsoring Organisations of the Treadway Commission (1994) *Internal Control Integrated Framework*. http://www.acca.com
12. Committee On Corporate Governance (1998) *Final Report*, Gee Publishing Co., January 1998.
13. Committee On Corporate Governance (1998) *The Combined Code*, J Gee Publishing Ltd, London, June 1998.
14. Elliott, M. W. *The Emerging Field of Enterprise Risk*, Marsk & McLennan Companies, Viewpoint, Number 2, Autumn 2001, http://www.mmc.com
15. Glover, S., Prawitt, D. & Romney, M. *Software Showcase*, **Journal of Internal Auditor**, Vol. 56, Issue 4.
16. IDM D.A.T.A. Solutions Limited, *Automated Fraud Detection V1.28: Fact Sheet*, March 2003.
17. Lanza, R. B., *Take my manual audit*, **Journal of Accountancy, Jun 98**, Vol. 185, Issue 6.
18. Le Grand, C. (2001) *Use of Information Technology in Auditing*, The Institute of Internal Auditors, 17/10/2001.
19. Leithhead, B. S. *In Touch with The Top*, **Journal of Internal Auditor**, December 2000, Vol. 57, Issue 6, p67.
20. Mack, P. R. 91971) *Planning Uncertainty, Decision making in Business & Government Administration*, John Wiley & Sons, U.S.A.
21. McCollum, T. & Salierno, D. *Choosing the Right Tools*, Journal of Internal Auditor, August 2003, Vol. 60, Issue 4, p32
22. McNamee, D. & SELIM, M. G., (1998) *Risk Management: Changing the Internal Auditor's Paradigm*, The Institute of Internal Auditors, Research Foundation, USA.
23. Mitchell, J. Personal Communication, London, August 6, 2003
24. Mullins, L. J., *Management and Organisational Behaviour*, Prentice Hall, 6th edition, 2002.
25. Outram, R. *The Cost of Catastrophe*, Journal of Internal Auditing, April 1997, p.12.
26. Paukowits, F. *Mainstreaming CAATTs*, Journal of Internal Auditor, February 1998, Vol. 55, Issue 1, p19.
27. Paul, L. W et al. *ERM in Practice*, Journal of Internal Auditor, August 2003, Vol. 60, Issue 4, p51
28. Price, D. *Personal Communication*, London, August 20, 2003
29. Pricewaterhousecoopers, *Global Financial Services e-briefing program, Taming Uncertainty: Risk Management for the entire Enterprise*, July 2002, http:www.pwc.com.
30. Raval, V. *Today's Information Systems Audits: Opportunities and Challenges*, **ISACA InfoBytes**, March 1998.
31. Rezaee, Z et. al., *Continuous Auditing: Building Automated Capability*, **Journal of Auditing**, Mar2002, Vol. 21, Issue 1, p147
32. Shields, G *Non-stop Auditing*, **CAmagazine**, September 1998, p39
33. Teixeira, T. *Risk Management and IT*, **Internal Auditing & Business Risk**, January 2001.
34. Teji, T. & Kettel, M. *Mastering risk beyond Turnbull*, **Internal Auditing & Business Risk**, March 2001.
35. The American Institute Of Certified Public Accountants, *Summary of Sarbanes-Oxley Act of 2002, Section 404: Management Assessment Of Internal Controls.*

36. The Institute Of Chartered Accountants In England & Wales (1999) *Internal Control - Guidance for Directors on the Combined Code*, London

37. The Institute Of Internal Auditors – UK And Ireland, *The Role of Internal Audit in Risk Management*, 25th of June 2002, http://www.iia.org.uk

38. The Institute Of Internal Auditors, (1999) *Standards for the Professional Practice of Internal Auditing*, IIA, USA

39. The Institute Of Risk Management (IRM), The Association Of Insurance And Risk Managers (Airmic), And Alarm The National Forum For Risk Management In The Public Sector, Risk Management Standard, http://www.airmic.com

40. Tillinghast – Towers Perrin, *Risk Management-A Practical Approach for the Insurance Industry, 2002 Benchmarking Survey Report.* (A)

41. Tillinghast – Towers Perrin, Miccolis, J & Sah, S *Risk Value Insights Creating Value through Enterprise.* (B)

42. Tillinghast – Towers Perrin, Miccolis, J & Sah, S *Enterprise Risk Management, an Analytical Approach.* (C)

43. TILLINGHAST-TOWERS PERRIN *Enterprise Risk Management; Trends and Best Practices, Editorial Summary*, **Journal of Internal Auditor**, July 2001, Vol. 59, Issue 4, p28. (D)

44. Weber, R. (1999) *Information Systems Control and Audit*, Prentice Hall, USA

INTERNET SITES:

http://www.acca.com
http://www.airmic.com
http://www.aon.com
http://www.bindview.com
http://www.icaew.co.uk
http://www.iia.org.uk
http://www.jebcl.com
http://www.mmc.com
http://www.pwc.com
http://www.theiia.org
http://www.tillinghast.com

Miss Effrosyni Papaefstathiou has an MSc in Internal Auditing & Management from the Business School, City University London and a BSc in Accounting & Finance from the University of Macedonia, Greece. Her academic field of interest deals with new applications for the internal auditing function. She can be contacted at **frpapaef@hotmail.com**

1. Strategic Risk Management – New Disciplines, New Opportunities (CFO, 2002).

2. Enterprise Risk Management in the Insurance Industry, 2002 Benchmarking Survey Report.

IT Outsourcing: Placing our Nation at Risk

Gordon Smith, President, CEO, Canaudit, Inc.

Reproduced from the *Canaudit Perspective* with the permission of Canaudit Inc.

As many of my clients know, I like to write controversial articles for the Canaudit Perspective. This issue is no exception and very well may be the most controversial article I have written. Last week I was reading the September 29, 2003 issue of Forbes Magazine, when an article by Robyn Meredith immediately caught my eye. The title was certainly unusual – "Giant Sucking Sound" **http://www.forbes.com/free_forbes/2003/0929/058.html** – not your normal Forbes title. As I read it, I quickly understood that there were major ramifications for auditors and security officers that were not covered in the article.

The article, which describes the continuing outsourcing efforts at EDS, mentions that 4,000 white-collar jobs (i.e. engineering, programming, and accounting) are being outsourced overseas each week. These are not low-skilled manual labor jobs. Rather, they are jobs that, in my mind, should not be outsourced overseas. Yes, I understand the economic issues. Andy in Mumbai (mentioned in the Forbes article) earns $1.25 per hour, is highly educated, and is certainly qualified to perform his helpdesk function. Certainly, the savings to the U.S. parent company are significant and make the company more competitive. While I am a strong believer in the free market economy, I also believe that outsourcing critical infrastructure jobs transcends economics and creates a clear and present danger to our country and our quality of life.

Overseas Outsourcing of the Helpdesk Weakens Security

Simple password resets may seem to be a trivial function to senior executives when they make the overseas outsourcing decision. In my mind, the ability to reset a password is very significant. By resetting the Administrator, DBA, or Superuser password on a system, the support person has the ability to take complete control of the server. If they have the ability to reset application passwords, such as PeopleSoft or SAP user accounts, then they may be able to gain DBA rights to the application or the database. Resetting normal user passwords may give the support person the ability to commit fraud. They could add fictitious employees to the payroll, change the automatic deposit information for employee and vendor electronic payments, change customer addresses to redirect mail, or divert shipments of expensive commodities.

The overseas staff may also have the ability to copy files and databases or perform data extracts. This will enable them to glean an organization's data, which could then be sold to a competitor. Customer data, once copied, could be used to feed an international identify theft ring. It could also be used to commit loan or bank fraud, obtain California drivers licenses (as if it is not easy enough already), or even apply for and be granted a U.S. Passport using the pilfered identity of a U.S. citizen.

I have been an auditor now for over a quarter of a century. One thing that I have learned is that when new business concepts and technologies are originally implemented, the incidence of fraud goes up for a short period of time until new controls are implemented. In the case of help desk outsourcing, I am concerned that just one fraud against a broad customer base of an organization, such as a large American bank, could result in massive electronic theft. After the cost of the fraud and the negative publicity resulting from the defalcation, will the company that outsourced overseas still have an economic gain from outsourcing?

System Development and Program Coding are Part of Critical Infrastructure

Here in the United States we have some of the finest military equipment in the world. We have the best fighter jets, aircraft carriers, submarines, missiles, and advanced weapons known to man. I am sure that the Advanced Tactical Fighter or the new aircraft carrier USS Reagan could have been built much cheaper overseas. In spite of the higher costs, these critical assets were built right here in the United States. Why? We want to ensure that the technology remains ours! We want to ensure that these weapons are built in a secure environment and that they are not sabotaged. The same holds true for the strategic petroleum reserves. These reserves are not located overseas. Our strategic petroleum reserves are stored right here in the continental United States. I am sure it would be cheaper to pay the overseas suppliers to store and deliver it to us "just in time," as we do with manufacturing components. However, it is just not prudent to do so.

Corporate America is rushing to outsource the development of new systems and maintenance of existing systems to countries with lower wages. Imagine the damage and destruction that would occur if customer bank account data, factory orders, or other mission critical databases were downloaded then erased using an administrator account. How large of a ransom would a large bank pay to successfully recover a stolen customer account database. How much would a credit card company pay to recover customer credit card balances that mysteriously were erased from the storage area network and all backups? All it takes to pull this off is some sleeper code placed into an application that can be activated at will. Since neither new code nor changes to code are reviewed line by line on a regular basis, it would be possible to insert the sleeper code into the programs and wait for the right moment. While this may seem to be an unlikely scenario, unless there are strong controls over outsourced programming resources then a data hostage situation could occur.

Outsourcing Facilitates Cyber-Terrorism

Now that we have covered fraud, let's take the scenario a step further. On September 11, 2001 we learned just how dangerous a few box-cutters could be. Now imagine the damage that could be done if a coordinated attack was made on Corporate America through sleeper code as mentioned above, time bombs, embedded viruses or worms, or other new techniques. The targets could be SCADA systems that control our electric and gas utilities, emergency 911 systems throughout the country, the New York Stock Exchange, airline reservation systems, order entry and shipping systems, hospital and medical applications, and the top 200 banks. Maybe a cyber-attack would shut down air traffic control systems or water purification plants. While this might be a good plot for a futuristic science fiction novel, I believe that with proper planning and coordination, overseas programmers could insert the required code into programs or database applications **AND THAT THE CODE COULD GO UNDETECTED**.

Many of the controls that were in place in bygone days, such as source code review, have disappeared. In many organizations, program change control is weak or nonexistent. I had a client who mentioned that the integrators had complete control over the project. They write the specifications based on client input; they engineer the solutions; and they code, test, and implement the software. At the end of the project, the integrator will turn the software over to the client upon acceptance testing. This is a fairly common occurrence. Our clients use integrators, because they do not have the skills nor do they want to hire and retain the skills to implement ERP systems. Some of the integrators outsource their coding overseas and this could lead to our downfall. (As an example of what can go wrong, review the case of Hershey: **http://www.cio.com/archive/111502/tl_hershey.html** and **http://www.philly.com/mld/philly/business/4416908.htm**.)

In my opinion, the likelihood that a cyber-terrorist organization could do significant damage increases as the software industry consolidates. There are fewer vendors, and more code is farmed out to overseas entities. Also, as in-house programming decreases, reliance on software vendors increases. Outsourcing product development is old hat for the larger software firms. They have outsourced this work for years. As more organizations standardize on these purchased software solutions, the risk of cyber-terrorism increases.

Data Ownership, Identity Theft, and Commercial Espionage

More data is being sent overseas or is accessed by employees who are not in North America. Some banks have moved part of their customer service operations overseas. Other banks are experimenting with expatriating our data. Your name, address, social security number, and bank balance can be viewed by individuals overseas. Many manufacturers have sourced their manufacturing operations in other countries to save on labor costs and the ever-increasing costs of complying with government and social obligations. The ability to build their products is in the hands of foreign entities. Now we are sourcing our information systems and customer management overseas! The outsourcers are talking directly to our customers through the miracles of modern Voice Over IP (VOIP) networks, documenting quality issues with our products, and learning how to effectively market to the North American consumer. High-tech companies which make some of the products we need for transportation, communication, computations, and many other products required to support our daily lives are outsourcing design, engineering, and even product testing overseas.

Let us look at what this means if we are an American technology company. We outsource design and engineering to Taiwan and Singapore, manufacturing to China, systems development to Pakistan, and information processing and customer service to India. Next we farm out backroom operations, such as accounting and procurement, to India or Eastern Europe. As companies outsource the majority of their operations overseas, it is only a matter of time until someone starts to silently and secretly acquire "control" of the Chinese manufacturing, the Indian information operations, and the engineering and research centers through a complex web of shell companies. In some cases, it may be through the purchase of these operations from the American parent; in other cases, they may acquire the intellectual capital of these firms.

By hiring the target company's overseas employees, they gain the knowledge required to compete against the American firm. By bribing existing staff members or hiring "consultants" to acquire new product designs before they are patented, this new business operation could outmaneuver the American company and capture market preeminence. The overseas combinations could pilfer existing product technology that can be "reengineered" to create a competing product. This would decimate sales and eventually the profits of those companies that are outsourcing critical infrastructure to overseas operations.

If this scenario becomes a reality, what will we have left in America? – High paid executive positions, low paid service industry jobs, and white-collar workers on unemployment insurance and welfare!

I recently discovered that the Final Four accounting firms are outsourcing or considering outsourcing the completion of tax returns overseas. Tax returns in the United States are considered confidential. The IRS strives to ensure our privacy. Now that this information is being exported, you can bet that at some point some of this confidential data will be disclosed. This confidential tax information could easily be used to commit fraud, identity theft, or to enable a terrorist to get a real U.S. passport using the name of a real U.S. citizen.

Gordon Smith is President and CEO of Canaudit, Inc.
He can be contacted at **gordon@canaudit.com**.

The Down Under Column

Bob Ashton

Two Firsts for Australia

1. Australian "Nigerian"

The evidence of what has become known as "Nigerian Letter Fraud", in the form of unsolicited emails, will be familiar to most people who log on to the Internet. It was recently reported in the Australian press that these scams had netted hundreds of millions of dollars. The perpetrators of such fraud represent themselves as Nigerian or other government officials asking for your help in placing large sums of money in overseas bank accounts.

The following information is provided by the FBI site, **www.fbi.gov**:

What is a Nigerian or "419" Fraud?

Nigerian letter frauds combine the threat, of impersonation fraud with a variation of an advance fee scheme in which a letter, mailed from Nigeria, offers the recipient the "opportunity to share in a percentage of millions of $$s", that the author, a self-proclaimed government official, is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers and other identifying information using a facsimile number provided in the letter. Some of these letters have also been received via email through the Internet. The scheme relies on convincing a willing victim who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several instalments of increasing amounts for a variety of reasons.

Payment of taxes, bribes to government officials and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and cheques that they received to impersonate the victim, draining bank accounts and credit card balances until the victim's assets are taken in their entirety. Whilst such an invitation impresses most law abiding citizens as a laughable hoax, millions of dollars in losses are caused by these schemes annually. Some victims have been lured to Nigeria where they have been imprisoned against their will, in addition to losing large amounts of money. The Nigerian government is not sympathetic to victims of these schemes, since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. The schemes themselves violate Section 419 of the Nigerian Criminal Code, hence the label "419 fraud".

In what is thought be to a world first, New South Wales Police have cracked what they alledge was a multi million dollar international "Nigerian fraud" syndicate operating out of Sydney. Officers seized nine houses in two countries, five cars, and several bank accounts and arrested a 39 year old certified Justice of the Peace and invalid pensioner, who they believe to be the brains behind the scheme which has tricked hundreds of people from Australia and elsewhere out of millions of dollars.

After receiving tip offs from Hungary and Canada, police staged a 4 month surveillance operation in which telephone and computer traffic was monitored, culminating in raids on three houses in which a number of computers and documents were seized.

The syndicate is believed to have taken more than $1.5 million from victims, including $1/2 million from a Saudi sheikh. Victims had been sent, in the form of faxes or emails, a notice which indicated that they had won a lottery or were the recipient of a large inheritance. They were then asked to pay an administrative fee of between $2,000 and $12,000 so the funds could be released into their bank account. Once the victims handed over the first amount, they were then asked for more.

The following is provided by the Internet Fraud Complaint Centre:

Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.

Do not believe the promise of large sums of money for your cooperation.

Guard your account information carefully.

But the best advice on how to deal with these emails is to delete them immediately.

It is not yet known whether such scams will become known as "Australians" in the future.

2. Skimming

A 29-year-old Malaysian citizen has been convicted in Australia's first card skimming case.

Skimming devices were installed with double sided tape at 36 ATMs to read the electronic information on the cards when they were inserted into the machines. The customer's PIN was also captured by the means of a pin head camera positioned to "shoulder surf" the victim. The data was re-written onto fake cards which were then used to empty the victims' accounts.

The perpetrator obtained more than $623,000 by this sophisticated fraud, and was able to transfer the bulk of this money to overseas bank accounts. This was done in transactions of less than to avoid the monitoring provisions of Australia's Financial Transactions Reports Act.

Mr. Ng will no doubt consider his visit to Australia as a profitable one, as he is likely to serve little more than 2 years. Much heavier sentences are routinely handed down in those Asian countries where this scam originated.

In The Bin

The Joint Committee of Public Accounts and Audit of the Commonwealth Government was recently dismayed to learn that sensitive government data, stored in wheelie bins by outsourcing contractor Telstra Enterprise Services (TES), had gone missing.

Backup tapes of email data from government agencies and departments, including the Prime Minister and Cabinet classified up to "protected" level had been stored in this unusual manner. The missing files are for the month of March 2003, which is considered to be particularly sensitive as this was when Australian troops were committed to Iraq. An Australian Federal Police investigation determined that there was no evidence to suggest that the absence of the tapes was due to criminal conduct, and that "the most likely explanation was that the tapes were accidentally disposed of as rubbish". When the losses were discovered TES staff did their best to recover them by scouring the local rubbish tip.

TES has not been penalized for this security lapse, but has agreed to upgrade its security arrangements. Hopefully wheelie bins will in future be used only for rubbish.

Further Stolen Computers

On the same day that the above enquiry learned of the wheelie bin storage arrangements, it was updated on the stolen Customs computers referred to in this column in the v.13 no.4 edition of this Journal.

The Committee was informed that 4, rather than 2, computers had been stolen in the August raid, but that the full extent of the losses were only discovered by Customs in October.

It is worrying that an internal audit of IT assets was conducted after the August break in, but the loss of the further 2 computers was not detected at that time.

Many observers believe that the extensive outsourcing of Government ICT services undertaken by the Howard government has resulted in a decline in national security.

Accountancy Age Personality of the Year

She may not be the most popular person at the European Commission, but it seems the tough-talking, no-nonsense approach that caused Marta Andreasen's suspension from her role as the commission's chief accountant has hit a resonant note with *Accountancy Age* readers.

Andreasen's award of *Accountancy Age* Personality of the Year rounds off a tough year for the whistle-blower that saw her face a barrage of criticism for her refusal to sign off the commission's 2001 accounts, followed by suspension and claims that she was attention-seeking and disruptive. However, her decisions at that time were largely vindicated by the emergence of new evidence to support her claims.

The suspension came on the back of her allegations that serious weaknesses existed in the EC's accounting procedures. Neil Kinnock, the commission's vice-president, claimed that Andreasen was not suspended for the criticisms she made, but because their relationship had broken down and she had decided to go public with her findings.

But, despite enduring an inquiry and threats of punishment, Andreasen was never subject to disciplinary proceedings over her allegations and in March, Jules Muis, the commission's internal auditor, reported that the whistle-blower's charges of fraud were 'factually substantive and correct'.

Her treatment at the hands of the EC wasn't even enough to put her off applying for Muis' job when he announced that he was to leave early next year.

The application was practically a challenge to Kinnock to forget the past and start a transformation of the commission's finances. 'If Kinnock really believes in reform, he would want to get someone into the (audit) job who is also prepared to continue reform,' she said in July. 'If not, it means that all he's been saying over the past three years is not true and that he's not in favour of reform.'

Followers of Andreasen's career will know that she is certainly no stranger to confrontation. Before her position at the EC, she had been appointed head of the accounting division at the OECD.

A clash with her then employer resulted in a bid to take the organisation to the European Court of Justice. She claimed that her human rights had been violated as she had not been given a 'fair trial' following allegations of racism and that she raised 'undue doubts' and unsupported 'alarmist allegations' in relation to OECD accounts.

Andreasen's win is a vote for those who stand up to immense forces and, while this award is by no means against the odds, she was up against some strong competition.

Press Review

Andrew Hawker

The Phishing Season

There is not much point in working hard on the security of your online services if you have users who are careless and gullible. This seems to be the message from several stories which have appeared in the UK press recently. For example, *The Guardian* (2 Aug) reported the results of a survey of office workers passing through Waterloo Station. 90% of those who were interviewed were willing to reveal their computer passwords in return for a cheap pen. The implication? If you are going to compromise the office system, you really should be demanding a much more expensive pen, or, at the very least, a pack of six assorted colour biros.

It is of course difficult to know if such reports actually help to get across any useful messages about good practice. The three key ingredients for any news report on computer crime are: (1) the whacky statistic (as above), (2) a case history, preferably based on the experiences of a poor down-trodden customer, and (3) the involvement of a Big Name. The best stories, naturally, combine all of these in an emotive mixture, and the Big Name is invariably cast as the villain. A natural reluctance to alienate readers means avoiding any suggestion that problems could be, at least in part, their own fault.

Throughout September and October, however, the papers have been carrying accounts of "phishing" attacks on banks, and the standard story line does not fit very well. Phishing involves tricking customers into revealing the identifiers and passwords which they use for access to online banking. The scam involves circulating official-sounding emails, which refer the reader to a bogus address or web site on which the personal details can be "re-registered". The email may also include a threat that failure to comply will result in the immediate closure of the bank account. The villains are unnamed hackers, the victims are customers who, dare it be said, are not always as careful as they should be, and the banks could argue that they are just as much the victims as anyone else.

As the number of bogus emails mounted, news reports followed a well-worn path, and homed in on attempts to defraud customers of Barclays Bank. Barclays are used to taking their place in the limelight. They know from past experience that being a market leader guarantees that any failure in their ATM or web site provision will make the headlines, certainly in the business pages. On 18th September, *The Mirror* reported that 13 bank groups around the world had been targeted for phishing, leading its story with the case of emails purporting to come from Barclays Customer Care. A couple of weeks later, The Telegraph highlighted a similar case of Rachel Hubbard, the recipient of a similar email from Barclays. Ms Hubbard was a bit puzzled, it seems, as she was actually a customer of Lloyds TSB at the time. By the end of October, it was apparent that quite a few big names in UK banking were being attacked. "Online bankers hit by e-mail scam" was the Telegraph's headline, over a report (28 Oct) that the bogus emails were being sent to customers of Natwest, Lloyds TSB, Nationwide BS, and the Halifax.

Having unveiled the scam, how effectively did the newspapers help their readers to cope with it? Well, one of the best bits of coverage, from this point of view, was in *The Mirror*. On 5th November, an article on online fraud ended with a list of simple rules for readers to follow, including advice on dealing with passwords. The coverage elsewhere was a bit more confused. For example, papers reported that some banks had closed their official web sites in response to the threat, a measure which seemed unlikely to help to protect customers who were being directed to bogus sites. However, as a warning message on the Lloyds TSB home page explains, one variant of the scam is for a link to the genuine URL to be embedded in the email, with an official-looking pop-up message being triggered at the same time, requesting the input of password and other personal details.

Generally, as might be expected, the broadsheets devoted many more column inches to phishing and all its implications than did the red-tops. Apart from *The Mirror*, hardly any coverage was provided in the tabloids. *The Sun*, for example, appears to have ignored the story completely. It may be that Internet banking is used much more widely by upmarket readers of *The Times* or *The Telegraph*, but this is surely a situation which is changing rapidly?

To more conventional crime .. On 9th September, several newspapers carried accounts of the conviction of three men for a fraud based on credit card numbers stolen from Heathrow Express. It was estimated that the team had made more than £2 million from their efforts. The fraud was based on a now familiar pattern of card numbers being passed over by an insider, and exploited via a mixture of deals involving alcohol, tobacco, drugs and pornography.

Finally, it seems that the mobile phone networks are catching up with the credit card providers. According to the Times of 1st November, T-Mobile and Cable and Wireless are jointly launching a scheme using "intelligent" software to monitor the pattern of mobile calls. Unlike credit card users, mobile subscribers are generally held liable for the full amount of any fraudulent use. It remains to be seen whether improved protection techniques of this kind will eventually result in better terms and conditions for the customers.

BCS MATTERS!

***Colin Thompson**, BCS Deputy Chief Executive, reviews some of the current BCS news items. Further information on these or any other BCS related issues may be found on the BCS web site (**http://www.bcs.org**)*

*Information is also available from Customer Services at The British Computer Society, 1 Sanford Street, Swindon, SN11HJ (e-mail to **marketing@hq.bcs.org.uk**)*

Moving Forward

The Extraordinary General Meeting, held in London on 23 September, produced a very emphatic vote in favour of proposals to change the BCS governance arrangements and membership structure.

The EGM on 23rd September was called to enable members to vote on proposals to change the existing BCS Charter and Byelaws. These changes, designed to modernise the governance and membership arrangements for the Society, were the subject of an intensive communication programme, under the banner of **It's Time to Move Forward** in the months leading up to the vote.

Over 30% of the eligible members took the opportunity to vote either in person at the EGM or by post in advance, and of these more than 97% were in favour. Both these percentage figures were above the level anticipated and overall the result represented a very substantial endorsement of the recommendation that the BCS Council made to the membership.

Since the proposals involve changes to the Royal Charter and the Byelaws, the approval of the Privy Council is required before they can be implemented. That approval has now been received and work is progress for the implementation of the most significant constitutional changes for the BCS since the grant of the original Royal Charter in 1984. These changes will include:

- A new Board of Trustees which will take over responsibility for the governance of the Society. Council will continue alongside the Trustee Board, and will appoint the trustees, but otherwise its responsibilities will be largely advisory.

- A new membership structure with professional membership separated from Chartered status. This separation will enable the BCS to offer MBCS at a much earlier career stage, on the basis of a much simplified entry process, whilst retaining the existing requirements and the more rigorous assessment process for the Chartered status.

The New Membership Structure

These changes mean that, from 1st May next year, the BCS will have 3 major membership offerings, apart from the Affiliate status which will be retained and enhanced:

1. *Ordinary Membership* – Those who have reached or are studying for a specified standard and have made a commitment to the code of conduct. This includes:

   i. Student membership for those on an approved course of study.

   ii. Companion membership (Comp BCS) for those from other disciplines involved in IT activity.

   iii. Associate membership as an entry grade for non-graduates (AMBCS).

2. *Professional Membership* – for those with a specified academic qualification (such as an accredited degree) and/or 2-5 years experience in the IT field, and who have made a commitment to the code of conduct.

3. *Chartered Membership* – for those who have satisfied further experience requirements and have been through the BCS process to accredit their competence and commitment. Such members will have the right to use a new chartered title, Chartered IT Professional, and to use the post nominal letters CITP in addition to MBCS or FBCS.

The link with the Engineering Council will be retained and suitably qualified chartered members will also be eligible for registration as Chartered or Incorporated Engineers. Existing Engineering Council registrants will of course be unaffected by the changes.

Speed of processing will be an essential element of the new professional grading and for most MBCS applicants we expect the process to take no more than a few days. This will be achieved in part by placing maximum reliance on 'trusted sources', including BCS Branches, Specialist Groups and individual Chartered members. It is the intention that applications carrying an endorsement from any of these sources will be accepted without the need for further significant validation. Arrangements are also being negotiated with some of the major employers of IT staff under which the companies will validate the accuracy of the application information as the basis for similar fast track processing.

Existing Members

The new structure will also mean grade changes for some existing members as shown in the following table:

EXISTING GRADE	NEW GRADE POST 1 MAY 2004
Affiliate	No Change
Student Member	No Change
Graduate Member	Associate Member (AMBCS) or Member (MBCS) depending on academic qualifications and experience
Companion (CompBCS)	No Change
Associate Member (AMBCS)	Member (MBCS)
Member (MBCS)	Member (MBCS) with chartered status
Fellow (FBCS)	Fellow (FBCS) with chartered status

Individual notifications will be sent to members affected by the change in advance of the implementation date. In the meantime, further information about the proposed changes can be found on the BCS web site.

A New European Qualification

Following enormous success with ECDL in the user area over the past few years, the BCS has now launched a new European entry level qualification for IT practitioners. EUCIP is an initiative of the Council of European Professional Informatics Societies (CEPIS) and is designed specifically for those who wish to gain a professional certification accepted throughout Europe..

The qualification is aimed at people with professional IT experience but who have no qualifications, individuals who have completed a non-IT education (at all levels), as well as younger students interested in entering the IT industry.

Successful achievement of the Certificate will demonstrate proficiency, and endorse the candidates' skills and capabilities in three key IT knowledge areas: Plan, Build and Operate. This allows candidates to demonstrate their expertise in each of the key areas. At each unit examination, the syllabus reflects a practical mix of up-to-date theory and current working practice. It aims to give a significant breadth and depth of knowledge and the ability to apply that knowledge in the workplace.

It is expected that the new qualification will be available through Further Education colleges next year. In the meantime, Parity Training has become the first UK organisation to be accredited by the BCS to deliver the new qualification.

Parity has achieved accreditation in all three core areas and has also been accredited as an official EUCIP testing centre.

A New President

At the AGM in October, John Ivinson handed on the BCS Presidency to Professor Wendy Hall CBE., one of the UKs leading computer science academics. Wendy is Head of Department at Southampton University and is only the second woman in the society's 46-year history to hold the post. (Steve Shirley was the other).

Prior to becoming Deputy President last year Wendy was the Vice President for Knowledge Services. During the course of her presidential year she will lead the society's initiative to improve quality control and professionalism in IT, by planning a series of events to increase awareness of the BCS among members of the public and Government departments. She also plans to encourage more women to join the society and hopes that in her capacity as President, she will be able to influence this sector.

And new Awards

More than 600 people, including Stephen Timms MP, Minister of State for e-Commerce. attended the first Awards presentation evening of the new-look BCS IT Professional Awards held at the Hilton Park Lane Hotel, London on Wednesday 24th September.

The programme incorporated the existing BCS Awards that date back 30 years as well as introducing many new categories for what has been recognised as the most ambitious and comprehensive IT Award programme ever mounted in the UK.

Sponsors for the new awards included Pricewaterhouse-Coopers LLP, BT, Brodeur Worldwide, Canon, Computacenter, DTI, IBM, Intersystems, Robert Walters, Marval Group, Mercury Interactive, Microsoft, Network Associates, PMP UK, Robert Walters, Siemens Communications and Syntegra. The awards were also supported by Computer Weekly, FT-IT Review, The Institute of Directors and The Worshipful Company of Information Technologists.

In ala there were nine excellence awards for individual professionals, four business achievement awards and five technology awards. There was something of a motoring theme to the latter category where winners included the *Prophet* system by *Speedtrap* and the *London Congestion Charging Scheme* by *Capita Business Services*. John Leighfield CBE, former AT&T Chairman won the first ever BCS Lifetime Achievement Award marking a lifetime's contribution to the IT industry.

Full details of the winners in all categories is available at **http://www1.bcs.org.uk/DocsRepository/05500/5589/awardswinners.htm**

New Product development

BCS are looking for skilled members to get involved with the development of new products and services. This opportunity would enable individuals to contribute actively to the development of innovative new products in line with current practices across the IT industry.

The Product Development Department is a key part of the HQ organisation, responsible for developing qualifications, services and software tools to support the education and training of IT professionals. It now requires the help of IT specialists with current or recent expertise willing to commit their time, energy and creativity.

Fees and expenses are paid, and the development projects are an opportunity for individuals to further their career, network and make a contribution to the future of the IT industry.

Further information is available from Malcolm Sillars (BCS Development Director) at **msillars@hq.bcs.org.uk**.

And Finally…….

This being the Christmas edition, may I take this opportunity, on behalf of all the staff at BCS HQ, to wish all readers a very happy Christmas and a prosperous New Year.

IT STAFF GET COMPREHENSIVE NEW INTERNATIONAL QUALIFICATION SCHEME

A major new pan-European qualification scheme both for people entering IT and for existing specialists seeking continuing professional development is being launched in the UK by the BCS.

The European Certification of Informatics Professionals (EUCIP) has been designed as an independent and international scheme for IT specialists in the same way that the hugely successful European Computer Driving Licence was developed as a standard test of IT user skills.

The EUCIP syllabus covers IT system planning, building and operation. The core syllabus takes around 400 hours of training, with a mixture of classroom courses, managed studying and assessments. After achieving the core certificate people will be able to gain more advanced qualifications in specialist areas such as network administration, software development and business analysis.

'The EUCIP Core Certificate certifies that the holder has a multi-disciplinary understanding of basic IT issues, ranging from IT strategy to system maintenance,' the BCS says.

The planning area of the syllabus, for example, covers more than 40 topics, including business processes, in-house development versus contracting out, project management, communicating with users, and copyright.

The building area ranges from system development tools to data modelling, software design methods, testing, documentation, and web page design.

There are no formal entry requirements for candidates, so the training and certification are open to anyone.

'In the short term the goal is to attract new practitioners into IT from other professions and from schools and universities, and also career changers, people with significant IT responsibilities, and non-qualified junior IT practitioners with narrow or scant IT background,' the BCS says.

'The long-term goal is to offer guidance and services to all IT professionals and practitioners and to support their needs for lifelong learning and continuous professional development.'

BCS chief executive David Clarke says, 'More than two thirds of the UK's workforce use IT but a significant number of people supporting them in IT departments still do not have any broad-based IT training or certification. EUCIP will be essential for candidates who want to document their competencies according to a European standard.'

He adds, 'By complementing the existing internationally recognised BCS short course vocational qualifications offered by the BCS Information Systems Examinations Board, the BCS Professional Examination, and the European Computer Driving Licence, EUCIP will underline the Society's role as the champion of the nation's computer literacy and skills programme and its commitment to delivering lifelong learning and IT professional development.'

The appeal of independent and international qualifications has been demonstrated by the European Computer Driving Licence, which is approaching 1 million registered people in the UK alone under the BCS' management, and the BCS IS Examinations Board, which has well over 19,000 IT people taking its certificates and diplomas every year.

The BCS is now appointing a network of accredited EUCIP training providers and testing centres.

EUCIP is an initiative of the Council of European Professional Informatics Societies, of which the BCS is a leading member.

Full details, including the syllabus and sample tests, are at **http://www.bcs.org/eucip**.

From the Cash Book

Jean Morgan – IRMA Treasurer

The main 'action' (if you'll allow me use that word where Treasuring is concerned) over this last quarter has been cheques flying in from all directions for membership renewals. And very welcome, they are too! Because renewals are still coming in fairly often, it's too early to know whether membership numbers are increasing or reducing. Membership is good value, with the cost staying the same again this year, so if you haven't renewed yet, please do so without delay. And if you're not a member and you're reading a colleague's copy, why not join us?

For the record, the total amount of income received for membership renewals between 1st August and 1st November is £3,770, or some 136 memberships, including corporates.

One thing that the Committee is looking at is the buffet provision at our evening meetings in London. Currently, the meetings are free to members. We are considering whether to increase the charge for non-members, although this may discourage prospective new members from coming along. If you have a view about this, please pass it on to one of the Committee members listed in the Journal.

EuSpRIG 2004

Risk Reduction in End User Computing

Thursday July 15th - Friday July 16th 2004

Universitaet Klagenfurt, Klagenfurt, AUSTRIA

Call For Papers

The European Spreadsheet Risks Interest Group (**www.EuSpRIG.org**) is issuing a Call for Papers for their fifth international conference on Spreadsheet Risks, Development and Audit Methods. The theme of this popular conference is 'Risk Reduction in End User Computing'. The programme will concentrate on:

- ***Raising the profile of the risks associated with spreadsheet use***
- ***The management and reduction of the risks associated with spreadsheet use***
- ***Spreadsheet development methods***
- ***Audit tools and methods***
- ***Productivity enhancements***
- ***Learning from alternative solutions and related approaches:***
- ***EuSpRIG are seeking the following types of submission:***
- ***Full academic papers (up to 5000 words)***
- ***Management summaries (up to 2000 words)***

It is expected that academics and students will contribute to full papers which will be reviewed by at least three referees selected from an international panel. Management summaries are predominantly expected from business people and practising professionals such as spreadsheet users, developers, auditors and accountants – all whom can contribute to the prevention, detection and correction of errors in spreadsheet models and applications. Two referees will review such summaries.

The best student paper will be honoured by a special prize.

Important Dates

Submit abstract to Programme Chair ***by 15th January 2004***
Submit full paper / management summary ***by 1st March 2004***
Acceptance Notification is to be received ***by 31st March 2004***

Timetable

The timetable will follow our established pattern of two half-days, to accommodate those travelling some distance, and will be published in detail in due course.

Submission Details

For submission instructions, details of formatting, handling of illustrations etc see related web page or contact David Chadwick at **programme@eusprig.org**. Draft papers and abstracts (in English) may be submitted in Microsoft Word or Rich Text Format to:
David Chadwick, Information Integrity Research Centre,
School of Computing & Mathematical Sciences,
University of Greenwich, 30 Park Row, London SE10 9LS, UK

EuSpRIG welcomes papers and management summaries from academics, accountants, IT professionals, auditors and interested business parties.

Further Information

For further information about EuSpRIG, including registration details, abstracts from previous symposia and ongoing research projects, please see our website at www.eusprig.org. To receive updates about the group's activities please send an email to our membership secretary: Grenville Croll: **membership@eusprig.org**.

HUMOUR PAGES

Accounting Jokes

On a sunny afternoon three accountants are standing near a tall pole and wondering about the height of the pole. First accountant, a Chartered one says, I do not think there is any authoritative guidance on how to measure the height of a pole. Second accountant, a professor at a university says, well, if we take a survey of similar locations and asked people about the height of poles, then we may be able to deduce the height of this pole, it will be a good enough estimate. The third accountant is a professor at an Oxbridge university. He confidently claims, if we measure the shadow of the pole under different conditions, then I can run a multivariate regression model and can give a very good estimate of the height. As this conversation is going on, an engineer is passing by, he stops and asks about their discussion. The accountants tell him, you probably can not understand this complex problem. The engineer persists and hears about the problem. He smiles, lifts the pole from the base, measures it, and says, "twelve feet and three inches," and walks off. The accountants look at him, laugh contemptuously and say in unison - "hell, we wanted to know the height of the pole and he tells us the length."

A very successful partner in a big four firm had a peculiar habit. He would go to his desk, open a locked drawer, look inside, lock the drawer again, and start his work. His subordinates knew that he hid the secret of his success in the drawer, they waited for the opportunity. One day when the partner had gone out of the city, the juniors decided to make a break. They broke into the drawer, breathlessly, and looked inside. There was one small piece of paper inside - it said - "left is debit and right is credit."

A Martian lands to plunder, pillage, and burn. The Martian goes up to the owner of the first house he sees and says "I'm a Martian just arrived from the other side of the solar system. We're here to destroy your civilization, pillage, and burn. What do you think of that?' The owner replies "I cannot express an opinion based on a hearsay evidence, I am a Chartered Accountant"

An auditor is hard at work, auditing an airline. The auditor cannot understand an excess fuel consumption on a Detroit to Erie route, for flight no. 420. The auditor calls the pilot and demands an explanation. The pilot replies "It was a late night, snow storm was raging, and I lost my bearings." The auditor demands a statement, "for what?" the pilot asks. The auditor tells him "for lost bearings."

The auditors have taken an inventory of thermometers held in a warehouse, in summer. The thermometers will be exported out of the country in January, and are kept under lock and key. In December, the auditors ask management to redo the inventory count. The management is surprised "Why? Nothing has changed." The auditors tell them "The inventory is overstated, in summer there is more mercury in the thermometers."

There was an expert accountant who was well versed in the game theory. He once hears that his intelligent niece, who is five years old, always takes a nickel, when a choice between a nickel and a dime is offered. He explains to his niece "You must understand, a dime is twice as valuable as a nickel, so always choose a dime." The niece tells "Uncle, but then people will not offer me any money."

An Indian Accountant's Theory of Reincarnation - if you are a good accountant, virtuous accountant, then you are reborn as an engineer. But if you are evil, wicked accountant, you are reborn as a psychologist.

One day in microeconomics, the professor was writing up the typical "underlying assumptions" in preparation to explain a new model. I turned to my friend and asked, "What would Economics be without assumptions?" He thought for a moment, then replied, "Accounting."

A science graduate asks, "Why does it work?" An engineering graduate asks, "How does it work?" An accounting graduate asks, "How much it costs?" A humanities graduate asks, "Do you want fries with that, Sir?"

An auditor is having a hard time sleeping and goes to see his doctor. "Doctor, I just can't get sleep at night." "Have you tried counting sheep?" "That's the problem – I make a mistake and then spend many hours trying to find it."

A *ccountant's Life —*
He was a very cautious man,
who never romped or played.
He never smoked, he never drank,
nor even kissed a maid.
And when up and passed and away,
insurance was denied.
For since he hadn't ever lived,
they claimed he never died!

A partner is discussing ethics policy with the staff accountant. He says "We take ethics very seriously around here. Remember, we are professionals not businessmen." The young staff accountant is impressed. The partner elaborates "Yesterday I received a check from a client. It paid $5,000 more than our bill. Immediately an ethical question arose, shall I tell it to other partners?"

An auditor is hard at work auditing a manufacturing plant. At the end of the shift he spots one worker who is always pushing a wheelbarrow covered with an opaque cloth. The auditor is certain something is fishy. He asks the security to check the wheelbarrow. Many surprise checks, security finds nothing. On the last day of the audit the auditor goes to the worker and asks, "Alright, I give up. I know you are taking something. I cannot prove it . I do not want to pursue it. I just want to know. What are you stealing?" The worker replies, "Wheelbarrows."

An Ode to Auditing

We test without apology
Both safety and ecology
And inventories, budgets, and production.
Checking scrap and sanitation,
Overtime, and transportation –
Not forgetting cost accounting and construction.
We test sales and check insurance
(EDP tries our endurance
As we audit payroll, cash, and simulation!)
We study management by objective,
Test controls that are defective,
And evaluate employee compensation.
We do sampling and regression
And there is a strong impression
We're responsible for catching all crooks.
We are really in our element
With research and development –
But thankfully we do not keep the books.
We check aircraft, trucks and motor cars,
And rockets that fly up to the stars,
And leases, loans – even personnel.
We examine engineering
Even salvage is endearing
And we check on records management as well.
There is nothing we can't verify –
There's nothing that escapes our eye.
Alert to all misconduct and to fraud.
We will go where others fear to tread
And as it has often been said,
"We are the eyes and ears of management and the Board."

by Lawrence Sawyer

Accounting Laws:

Trial balances don't
Working Capital does not
Liquidity tends to run out
Return on investments never will
Bottom line is only the tip of the iceberg.
Those who live by the bottom line shall die by the bottom line.
Accountants have a vacuum-tube mind in a solid state world.
Accounting: A bunch of numbers running around looking for an argument.
A fool and his money are soon audited.
Cash in hand means bill in the mail.
If you need accounting to prove it, it was probably not true in the first place.
Obviously accounting pays, otherwise there would be no accountants.
There is nothing more permanent than temporary account.
Accounting will prove anything, even the truth.
Accountants carry their calculations to two decimal points only to prove that they have marvellous sense of humour.
Accounting proves that money is the least viscous of all substances.
Artificial hearts are no big deal; they've been around since the first accountant.
An accountant is a man hired to explain that you did not make the money you did.
Accountants are witch doctors of the modern world.
Accounting is economics without assumptions.

Member Benefits

Mark Smith

IRMA is pleased to announce that we have negotiated members' discounts on the purchase of a number of software packages:

Product	*Discount Negotiated*	*Supplier*
Caseware Examiner for IDEA (mines security log files for Windows 2000, NT, XP)	**15%**	**Auditware Systems (www.auditware.co.uk)**
IDEA (Interactive Data Extraction and Analysis)	**15%**	**Auditware Systems (www.auditware.co.uk)**
Wizrule (data auditing and cleansing application)	**20%**	**Wizsoft (www.wizsoft.com)**
Wizwhy (data mining tool)	**20%**	**Wizsoft (www.wizsoft.com)**

We are looking to extend this range of discounts to include additional software or other products that our members may find beneficial. If you have any suggestions for products we could add to the list, please contact our Members' Benefits Officer (Mark Smith, **mark.smith@lhp.nhs.uk**) who will be happy to approach suppliers.

IRMA
INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	John Bevan	john_bevan@ntlworld.com
DEPUTY CHAIRMAN	Alex Brewer	alex.brewer@morganstanley.com
SECRETARY	Siobhan Tracey	siobhan.tracey@booker.co.uk
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Celeste Rush	rushlse97@aol.com
JOURNAL EDITOR & SECURITY PANEL LIAISON	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@!internetworking4u.co.uk
EVENTS PROGRAMME MANAGER	Graham Devine	graham@grahamdevine.me.uk
EVENTS PROGRAMME CONSULTANT	Raghu Iyer	raguriyer@aol.com
LIAISON - IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON - LOCAL AUTHORITY	Peter Murray	cass@peterm.demon.co.uk
LIAISON - ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wally Robertson	williamr@bdq.com
ACADEMIC RELATIONS	David Chadwick	d.r.chadwick@greenwich.ac.uk
	David Lilburn Watson	dlwatson@bcrm.co.uk

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	members.irma@bcs.org.uk janet@carliam.co.uk
LIAISON - KPMG	David Aurbrey-Jones	david.aubrey-jones@kpmg.co.uk

OR VISIT OUR WEBSITE AT **www.bcs-irma.org**

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

Reach the top professionals in the field of EDP Audit, Control and Security by advertising in the BCS IRMA SG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, contact John Mitchell on 01707 851454, fax 01707 851455 email john@lhscontrol.com.

There are three ways of advertising with the BCS IRMA Specialist Group:

The Journal is the Group's award winning quarterly magazine with a very defined target audience of 350 information systems audit, risk management and security professionals.

Display Advertisements (Monochrome Only) Rates:

- Inside Front Cover £400
- Inside Back Cover £400
- Full Page £350 (£375 for right facing page)
- Half page £200 (£225 for right facing page)
- Quarter Page £125 (£150 for right facing page)
- Layout & artwork charged @ £30 per hour

Inserts can be included with the Journal for varying advertising purposes, for example: job vacancies, new products, software.

Insertion Rates:

For inserts weighing less than 60grams a flat fee of £300 will be charged. Weight in excess of this will incur additional charges:

- 60-100grams: 14p per insert
- 101-150g: 25p per insert
- 151-300g: 60p per insert
- 301-400g 85p per insert
- 401-500 105p per insert

Thus for an insert weighing 250g it would cost the standard £300 plus weight supplement of £210 (350 x 60pence) totalling £510.

Discounts:

Orders for Insert distribution in four or more consecutive editions of the Journal, if accompanied by advance payment, will attract a 25% discount on quoted prices.

Direct mailing

We can undertake direct mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our members plus a handling charge.
Access Charge £350. Please note photocopies will be charged at 21p per A4 side.

Personalised letters:

We can provide a service to personalise letters sent to our members on your behalf. This service can only be provided for standard A4 letters, (i.e. we cannot personalise calendars, pens etc.). The headed stationery that you wish us to use must be received at the Office at least ten working days before the distribution is required. Please confirm quantities with our advertising manager before dispatch. If you require this service please add £315 to the Direct mailing rates quoted above.

Discounts: Orders for six or more direct mailings will attract a discount of 25% on the quoted rates if accompanied by advance payment

Contacts

Administration

Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: janet@carliam.co.uk
Website : www.bcs-irma.org

BCS IRMA Specialist Group Advertising Manager

Eva Nash Tel: 01707 852384 & 07973 532358
E-mail : eva@nash141.freeserve.co.uk

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

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)
E-mail:
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 IRMA"AND RETURN WITH THIS FORM TO

Janet Cardell-Williams, IRMA Administrator, 49 Grangewood, Potters Bar, Herts EN6 1SL. Fax: 01707 646275

ADDITIONAL CORPORATE MEMBERS

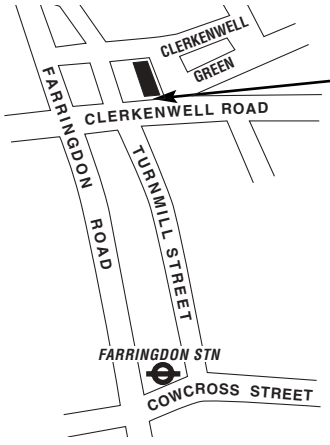
INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
E-mail:
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

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

Venue for
Full Day Briefings



Old Sessions House
Clerkenwell Green
London EC1

Venue for
Late Afternoon Meetings

KPMG
8 Salisbury Square
London EC4