Managing Risk to Enhance Stakeholder Value

The mission of the International Federation of Accountants (IFAC) is the worldwide development and enhancement of an accountancy profession with harmonised standards, able to provide services of consistently high quality in the public interest.

This booklet was prepared by the Financial Management Accounting Committee (FMAC) of IFAC. The strategy of FMAC addresses:

- Thought leadership is expanding the field of practice known as management accounting;
- Sharing of best practice in this field globally; and
- Assisting developing countries as they explore the benefits of management accounting.

Finally, my thanks to those members of FMAC who organised this project to bring these leading articles and interviews to our attention. This group consisted of:

Bill Connell, Director of Risk Management, BOC group plc
Raymond G Darke, Executive-in-Residence, DeGroote School of Business, McMaster University
Professor Bill Birkett, University of New South Wales
John Petty FCPA, National Vice President CPA Australia
Richard Mallett, Technical Director, Chartered Institute of Management Accountants

Bill Connell
Chairman

Members of the Financial & Management Committee

Santiago C Lazzati, Argentina	Gerhard Prachner, Austria	David Jeffries, Australia
Raymond G Darke, Canada	Patrick Rochet, France	Srinivasan Ramanathan, India
Ghasem Fakharian, Iran	Rodolpho Di Dato, Italy	Yeo Tek Ling, Malaysia
Peter A M Sampers, Netherlands	Muhammad Aslam, Pakistan	Zein El Abdin El Boraie Ahmed, Sudan
Recep Pekdemir, Turkey	***Bill Connell, Chair, UK***	William L Brower, USA

The FMAC welcomes any comments you have on this booklet. Comments should be sent to:

Technical Manager, International Federation of Accountants, 535 Fifth Avenue, 26th Floor, New York, New York 10017-3610 USA
Fax: +1 212-286-9570 E-mail: edcomments@ifac.org

Copies of this paper may be downloaded free of charge from the IFAC website at www.ifac.org and from the CIMA website at www.cimaglobal.com.
Hard copies are available from CIMA Publishing on: 0208 849 2277/2229/2270 or www.cimapublishing.com

IFAC ISBN 1 88746 493 X
CIMA ISBN 1 85971 563 X

Contents

* These articles are based on interviews conducted by leading accountancy journalist, Robert Bruce.

Risk Management

Overview

Bill Connell FCMA

The 2002 theme booklet from IFAC's Financial and Management Accounting Committee (FMAC) focuses on the theme of Risk Management from both the traditional review of the financial risks of a company and the emerging application of risk management techniques in the areas of strategy, reputation and people.

The Financial and Management Accounting Committee of the International Federation of Accountants (IFAC) explores emerging trends and seeks to represent contemporary best practice in the domain of professional accountants in business. This, and recent FMAC publications that have covered topics such as *A Profession Transforming: From Accounting to Management* (Study 11) and *The Role of the Chief Financial Officer in 2010*, are aimed at executives and senior finance professionals who are responsible for leading their businesses forward. In this publication, we have again canvassed the views of leaders in the field of strategy and risk management, and their views are described through the faciliatation of the leading accountancy journalist, Robert Bruce. We thank them for sharing their insights and their candid comments. After the depth of material on risk management from an audit based perspective, this publication refreshingly provides views on risk management from accountants and others working in business.

In the first article – 'The Practical Application of Corporate Governance and Risk Management', a framework for understanding corporate governance is laid out and the role of risk management is explained.

> 'many organisations are now looking to better align their corporate planning and risk management activities to promote the selection of targets that are both stretching and achievable'
>
> 'The importance of risk management has advanced over the last few years with many organisations understanding that they have to take more risk if they are to generate value, and that all employees have a part to play in achieving this. Just as directors need to provide challenge on risk issues, clear ownership and accountability for risk needs to exist at all organisational levels'.

This theme is then picked up in the other articles. In the BOC case study (Risks and Strategy) 'The real plus is knowing that people are thinking in a risk management way automatically' is how Tony Isaac, the CEO, puts it. 'Risk becomes a normal part of the management process and people can then take more risks because they understand them and manage them through.' The article explains how the risk management professionals facilitated and challenged the strategy process and emphasised the theme of getting positive plans in place to improve the probability of achieving strategic objectives.

'Corporate governance has made risk management very topical, but you cannot go through the risk management process for those reasons. You have to do it because it helps the business. If you go through the process of risk management for corporate governance reasons you simply end up with bureaucracy' is the BOC advice that is worthy of full consideration when embarking on this journey.

This theme is continued in the article on managing business interruption. Kevin Hayes, MD and CFO of Lehman Brothers describes how they managed after the events of September 11.

'Historically, business continuity planning was about data recovery. Today, it is recognised that there is a need to integrate it into everyday business processes so that crticial elements of the business continue working in all circumstances.'

The articles on the implementation of risk management in the public sector in Australia and the UK reinforce many of the issues being raised in other articles but against the different objectives of a government organisation.

Other themes that emerge are the importance of employees and the change in culture in organisations. Kevin Hayes describes how changes in technology enable home working which helps following a crisis such as September 11. Steve Marshall in explaining the effects of reputational risk which put Railtrack in the UK 'in the top three daily television news items for 45 consecutive days' goes on to explain the importance of staff morale. 'Staff are the most powerful ambassadors you can have. If honest and positive views are being expressed rather than the pessimistic tones of a workforce whose moral has gone, it can make a huge difference. It does have a powerful effect.'

The subject of reputational risk takes into account all of the organisation's stakeholders and this is described in the Railtrack article. But reputational risk is not just about major disasters. In the Unilever article 'An internal audit best practice case study' this is well recognised when looking at how organisations have changed. 'We were still focusing too much on the profit and loss account and the balance sheet and on fixed assets. They were important but those areas are not what kills businesses now.' Professional accountants in business must take a multi-dimensional view of their business and discuss risk management in the context of the strategic planning process in their company.

Other articles address the important role of internal auditors. 'The non executive directors are looking for more assurance from whatever source they can get and internal audit is at the heart of that' and the growing need for disclosure of risks. The article by Stathis Gould, who I am indebted to for his project co-ordination of this theme booklet, considers the current level of risk disclosure, looks to the motivation for better disclosure, and gives clear signposts for the future. 'The crucial issue for all stakeholders is that internal procedures actually add value and inform the business. As we are seeing with corporate social responsibility reporting, leading companies will want to distinguish themselves from the rest of the pack. For these companies, the goal will be for a seamless interface between management accounting, external reporting and investor needs.'

Other articles on risks in the acquisition process, capital structure risk and dealing with information risk are excellent examples of the many strands of risk management facing organisations.

This theme booklet has struck a rich vein of best practice in this important and emerging area. The contemporary view of risk management involves treating risk in the context of business strategy and senior finance professionals and chief risk officers are responsible for moving the agenda away from risk minimisation to risk optimisation so that the process drives performance and creates shareholder value. This is opposed to the traditional view, which has connotations of loss prevention and transfer through insurance mechanisms and the hedging of financial risks with derivatives. 'A Profession Transforming: From Accounting to Management' has never been more true.

Bill Connell
Chairman, IFAC's Financial and Management Accounting Committee
November 2002

Risk Management

Performance from Conformance –

The practical application of corporate governance and risk management

Richard Sharman **and** ***Tim Copnell, KPMG***

Richard Sharman is the Director responsible for the Enterprise Risk Management practice in London and is jointly responsible for managing and developing KPMG Enterprise Risk Management Services in Europe. A holder of an MSc in International and Corporate Finance, Richard specialises in designing and implementing enterprise-wide risk management strategies, in particular identifying and measuring the impact of risk on organisational strategies, processes, cultures and behaviours.

Timothy Copnell is the Director in Charge of KPMG's UK Audit Committee Institute. He qualified as a chartered accountant in 1989 and joined KPMG's Department of Professional Practice in 1993 where he took responsibility for corporate governance matters.

Letter rather than spirit

From Cadbury to the Combined Code, from Viénot to the new German Code, the corporate governance reforms of the last decade have systematically formalised the manner in which companies are governed. Given the current spate of restated financial statements, missed earnings projections, and high profile corporate failures, the jury is still out as to how effective such reforms have been.

What can be said of the explosion of corporate governance-related guidance observed during the 1990s is that it prompted a commitment of increased time and investment in risk management but in the majority of cases organisations continued to treat risk management as a discrete exercise. Ultimately this failed to focus risk management activity on the strategic objectives that lead to improved organisational performance and, in turn, improved shareholder value. Observing the letter rather than the spirit of corporate governance guidance is something organisations should be wary of.

So what exactly is corporate governance and what is its relationship with risk management? Furthermore, how are organisations supposed to meet the expectations of their stakeholders in these areas and, the two not being mutually exclusive, actually drive performance benefits while doing so?

So what is corporate governance?

Put simply, corporate governance is the system and processes by which entities are directed and controlled to enhance performance and sustainable shareholder value. It concerns the effectiveness of management structures (including the role of directors), the sufficiency and reliability of corporate reporting, and the effectiveness of risk management systems.

During the last few months, the issue of corporate governance has been dominated by reactions to three major events: the collapse of Enron and the rash of other high-profile financial restatements; new risk perceptions due to the tragic events of 11 September 2001; and the economic downturn and its impact on financial reporting.

Each of these events has resulted in significant shareholder interest in corporate governance and how it might be improved to minimise similar risks at their companies. Boards are under increasing pressure to become more accountable, transparent and responsive to stakeholders.

A framework for understanding corporate governance

What follows is a defined governance framework focused on value creation – a framework to ensure the spirit of corporate governance is followed to deliver both conformity and performance improvement. Once boards fully understand their stakeholders, they will be better able to ensure governance effectiveness and accountability and thus add value to the organisation overall.

We explain how this is practically achieved in greater detail below as we deal with the five pieces of the governance jigsaw individually:

1. Board operations

Effective board operations are critical to the development of a strong governance structure. The skills and experience of the board must remain relevant to the company's needs, whatever the standards, culture, and markets to which it is subject. Boards should take steps to ensure that they continue to have the appropriate mix of skills and levels of experience as conditions change. Periodic self-evaluation, preferably facilitated by an independent third party, will help them meet this important goal.

Ultimately, the quality of the financial reporting, risk management and internal control structures that support the discharge of governance responsibilities will be rendered meaningless if the board operates ineffectively. Central to effective governance is the level at which risk and control issues are discussed and the frequency and standard of that discussion. In the current environment non-executive directors are being asked to question the level of challenge they currently provide to the executive. In response they are asking for improved information on the risks the organisation faces, the controls in place to manage these risks and the process by which this information is arrived at and updated.

However, risk clearly does not stop once you get past the operational tiers of an organisation. Risks associated with succession planning and remuneration arrangements are repeatedly highlighted by the financial markets and yet are rarely identified or communicated effectively. The level of challenge at board and sub-committee level and an appetite to confront such issues are essential to effective board operations.

Questions on the level of challenge should not be reserved specifically for non-executives. An example is the way in which many organisations have sought to better discharge their governance responsibilities through establishing dedicated risk management committees.

2. Strategy development

The board should seek to ensure that the organisation is sufficiently agile to be able to respond to changing circumstances and take advantage of relevant market opportunities even as it continues to pursue its planned goals and objectives. Aligning board and management efforts is an important first step — one that will help enable both groups to work co-operatively to achieve strategic aims and ultimately add value for stakeholders.

Effective strategy development observes how key risks are managed and how risk influences business performance in the same way that the taking of opportunity can be seen to. Managing and reporting on risks outside the context of the organisation's business objectives is at best interesting, at worst a waste of time. As a result, many organisations are now looking to better align their corporate planning and risk management activities to promote the selection of targets that are both stretching and achievable and to assist in the subsequent dialogue at all levels on actual results.

3. Corporate culture

Efforts to ensure ethical behaviour and to protect an organisation's reputation are an important part of the governance framework. A culture that condones negligent or even mediocre behaviour puts the company's reputation at risk. Moreover, where appropriate standards of conduct promoting and maintaining integrity are not embedded within a company, there is a heightened risk that employees' behaviour and the information they produce become unreliable. The board must help ensure an appropriate tone at the top.

The importance of risk management has advanced over the last few years with many organisations understanding that they have to take more risk if they are to generate value, and that all employees have a part to play in achieving this. Just as directors need to provide challenge on risk issues, clear ownership and accountability for risk needs to exist at all organisational levels.

As organisations seek to support high performance and increased risk-taking, some are now including the evaluation of employee attitudes to risk in their performance appraisal process, firmly positioning risk management as a component of induction and ongoing management training.

4. Monitor and evaluate

No matter what their level of focus, boards should recognise that what gets measured is what gets attention. Therefore, they need to ensure they understand what management should be doing and assess whether those activities are being managed and measured. The reports the board receive should reflect this broad measurement perspective. How well management has met the organisation's financial goals should be just one aspect of the board's evaluation. The board should also ensure that the

combined scope of internal and external audit is such that it is able to provide greater assurance that management has adequate governance systems and processes in place to protect shareholder value.

Inseparable from the development of organisational strategy is the monitoring and evaluation of subsequent performance. When reporting on risks to business objectives many organisations continue to confuse quantity of reporting with quality of reporting.

A growing number of organisations are appointing a chief risk officer to provide leadership, direction and co-ordination of organisational risk management activity. The chief risk officer does not directly 'own' responsibility for managing specific risks but operates in a consultative/collaborative role supporting the board, its sub-committees and key operating and functional management. The role seeks to improve consistency and accessibility of risk information at all levels of the organisation as well as improve the standard of discussion and challenge at board and management levels.

As organisations better align their planning and risk management activities and the consistency of their risk reporting, they are also improving the means by which they measure performance to corporate objectives. For many, the next step is the integration of information on key risks with these methods for monitoring performance since both seek to measure the likelihood of achieving the same corporate goals.

5. Stewardship

Board members are accountable to shareholders. Accountability – including all the issues surrounding disclosure and transparency – is what provides the legitimacy to the classic model public company. Shareholders elect directors to run companies on their behalf – *ipso facto*, boards are accountable to shareholders for their actions. Boards should engage in a two way dialogue with their key stakeholders and use their acquired knowledge as part of their strategic planning and risk management process. Decisions based on a better understanding of stakeholders' needs reduces the risks associated with the external environment and helps secure competitive advantage.

Elsewhere we have discussed the improved alignment of organisational performance and risk information to better measure performance against objectives. The development over recent years of environmental, sustainability and social responsibility reporting represents one way in which organisations are responding to stakeholder concerns on risk. In many cases the risks and how they are actively managed are acutely linked to organisational sustainability – an example being that of mineral reserves for energy organisations. The ways in which these organisations look to develop and report on alternative energy sources explains to stakeholders their own plans for longevity as well as that of the planet.

It is foreseeable that developing demands for disclosure and transparency and the desire to create competitive advantage will lead to increased reporting on other areas of risk and organisational efforts to manage them.

Time for companies to assess the true value of corporate governance towards performance

The true value of good corporate governance lies in its contribution to both business prosperity and to accountability. In the current environment it is all too easy to forget the former. Nevertheless, business leaders and shareholders alike must ensure that undue concentration on aspects of accountability does not destroy entrepreneurship and ultimately value.

Recent events have brought about heightened awareness of governance issues and efforts to improve and demonstrate high governance standards. Such efforts should extend throughout all five of the board's major focus areas — board operations, strategy, corporate culture, monitoring and evaluation, and stewardship. Correspondingly, and perhaps unsurprisingly, developed risk management activity clearly assists in meeting and exceeding stakeholder expectation in all of these five areas.

Ultimately, demonstrably strong corporate governance is essential to preserving reputation, investor confidence, access to capital, employee satisfaction, customer loyalty, and long-term sustainability. Poor or inadequate governance, by contrast, will not maximise shareholder value, but it will attract the attention of those who see reforming governance as a means of increasing value.

Risk Management

Risks and Strategy

A BOC case study

An interview with *Tony Isaac FCMA, Chief Executive Officer, BOC* and *Bill Connell FCMA, Director of Risk Management, BOC*

Tony Isaac is Chief Executive Officer of the BOC Group, one of the world's largest industrial gases companies. He joined as Finance Director in 1994, having previously held similar positions with Arjo Wiggins Appleton and GEC Plessey Telecommunications. He is a non-executive director of Exel plc and International Power plc.

Bill Connell, Chairman of IFAC's Financial and Management Accounting Committee, is Director of Risk Management for the BOC Group plc after previously being Director of Financial Management, Industrial and Special Products.

The BOC Group Plc

BOC is an industrial gases and vacuum company which operates in over 50 countries. It has a turnover of £5.6 bn and has over 40,000 employees.

The changing attitude towards risk management

Over the last year BOC, the global industrial gases giant, has undergone a transformation in the way it deals with risk. And if you were in any doubt over the benefits of such an exercise you only have to listen to the BOC chief executive, Tony Isaac, and the director of risk management, Bill Connell.

'The real plus', Isaac tells you, 'is knowing that people are thinking in a risk management way automatically'. Or as Connell puts it: 'It becomes a normal part of the management process'. They both agree on the advantages that accrue. 'From an initial scepticism', says Isaac, 'the organisation is grabbing it for themselves'. Connell underlines the point. 'People become increasingly comfortable with the risk', he said. 'People can then take more risks because they understand them and can manage them through'.

It has been a steady process of both changing and then embedding the culture. The roots go back to a view that risk management needed to be firmly embedded within the organisation and the process started in July 2001 with a workshop for the board of directors. This outlined the process ahead and was based on shareholder value as a major driver. The new strategy was then created across a six-month period and presented to the board in March. 'From September to February', said Isaac, 'we did a total re-review of all of our strategy. It was time to look at it again'.

The original workshop reviewed the value of future growth options. This focused on the risks and opportunities of growth projects and internal and external strategies and the overarching risks which might be faced by the existing business model. It produced a system which created a continuous loop. It started with strategy, identified the risks to the strategies and determined the preferred risk treatments. From there the loop progressed through the execution of the strategies and the communication of the risk and risk treatments connected to a share price based firmly on the estimation of future earnings and an assessment of core competencies. This could then loop back into the creation of future strategies. It would be a virtuous circle.

But its creation meant the changing of mindsets and the asking of hard questions. 'We were', said Isaac, 'questioning everything in our existing strategy'. BOC has three major lines of business, eighteen business units and several specialist units. It was to be a difficult but rewarding task.

The process

'We used the format of risk workshops', said Isaac, 'evaluating what our competitors were doing, for example. What they could do in each market, and what their market entry strategies might be? What they might do? What their consolidation strategies would be'? Then the consequences could be evaluated. 'We needed to ask what organisational changes were needed', said Isaac. It was a question of questioning everything. 'Members of the executive management team,' said Connell, 'suggested the risks and then prioritised them before talking through what plans they might have against those risks'.

Initially this process is hard and can provoke gloom. 'The first discussions', said Connell, 'always produce what can go wrong. They concentrate on the downside while it is much more important to make sure things go right'. Initially, as Connell put it, 'the mindset is too much on the "bad things" side'.

This is where the risk management department has to provide the tools to turn the views around. Connell urged everyone to 'think ahead three years and imagine writing an obituary. Then analyse what would have stopped you achieving what you wanted to achieve'. It is a very useful way of looking at obstacles and opportunities. 'For example', said Connell, 'people could say that it would involve too much organisational change. So we would turn it round and ask how do we gain the tools and techniques to have effective organisational change'.

Embedding a new culture

Another stumbling block was the whole question of people and change. 'How do we get people to be comfortable with change?', asked Connell. 'You need good plans and that helps people understand the risks and achieve the strategy. It is all a question of identifying risks and then getting positive things in place to help', he said.

'We produced a strategy which made sense', said Isaac, 'and we reviewed it in detail with the senior team'. For Isaac the key to the next step was 'what were the things we had to do well to achieve the strategy?'. The upshot was that the team foresaw six major risks. The first was what BOC's competitors were going to do. The second concerned Asia, where much of the planned future growth was going to be. The third was dealing with the group's semi-conductor business. The fourth was a financial strategy. 'If our short-term profit growth was around the issues of pricing and productivity', said Isaac, 'how could we accelerate it?'. The fifth concerned economics. 'We tested our economic assumptions', said Isaac. 'We asked what impact would our assumptions about global growth of GDP have on our plan'. The sixth area was the organisational changes which had to be made to underpin some of the initiatives. This was a question of: 'How much change management could the group and the businesses cope with', said Isaac.

The crunch session involved two-and-a-half days with the board. 'It was a very good session', said Isaac. 'We gave them a lot of pre-reading so there was plenty of debate'. This was then followed by a process which spread the strategy through the top hundred senior people in the group. 'Two-thirds of our six-monthly management workshop was given over to the strategy', said Isaac. 'Since then there have been detailed workshops around the strategy', he said, 'and now there are milestones which can be monitored and which we are using throughout the business'.

The test lies in the long-term achievements ahead. 'Time will tell how successful it will be', said Isaac, 'but it means more and more concentration on achieving those milestones. In the past there has not been enough strategic buy-in or long-term monitoring'.

Outcomes

Isaac paid tribute to the contribution that the risk management team had made to the process. 'The risk management team had an important role in the strategy workshops', he said. 'They played devil's advocate, particularly when evaluating what competitors might do'. Connell agreed. 'My team are facilitators', he said. 'They need to be close enough to understand but be independent enough to make the challenge'. This did not always go down well. 'The challenge process was initially seen as confrontational', he said. 'But it quickly moved to an acceptance that it was helping people go forward. People had to present to senior management', he said, 'which focused their minds'.

For Isaac there are many lessons. 'Risk management has made us much more aware of what we need to do in terms of acquisitions, for example', he said. 'It made us look again at the generics of acquisitions - how good we think we are at evaluating, screening, negotiating and implementing, for example. It has increased an understanding that acquisitions take a lot longer to implement and you understand better at what point you walk away. We have also learned more about what is required and in particular the basis of collaboration with partners', he said. Levels of internal training have also been increased.

For Connell the process of coming up with an analysis of the overarching risks and the planning of their mitigation has been valuable. He also stressed the embedding process. 'You can tell if it's working', he said. 'One person will tell you we can do this. Another will tell you: "I don't think I can get a plan out in time for the meeting". It is easy to tell where the process is embedded'.

Connell also counsels against going through the process for the wrong reasons. 'Corporate governance has made risk management very topical', he said. 'But you cannot go through the risk management process for those reasons. You have to do it because it helps the business. If you go through the process of risk management for corporate governance reasons you simply end up with bureaucracy'.

'Risk management', concluded Isaac, 'is a discipline. Once people in the businesses have been exposed to the pluses and minuses, they want to embed the discipline themselves in what they do'. The BOC Group is now employing the principles in every project and every acquisition. 'Once you have immersed yourself in a risk management workshop', said Isaac, 'you can do it yourself'.

And in the end it does embody some very fundamental points. For Connell it is a question of reconciling two perspectives. 'It is a question of making sure bad things do not happen', he said, 'and making sure that good things do happen. It is a question of identifying what could go wrong and what must go right'.

Risk Management

Managing Business Interruption

An interview with *Kevin Hayes, Managing Director and International Chief Financial Officer, Lehman Brothers*

Kevin Hayes has been with Lehman Brothers for seven years starting as the Global Fixed Income Controller. In 1999, he became the Global Capital Markets Controller, and in January 2002, was appointed the International CFO for Europe and Asia. Prior to Lehman Brothers, Mr Hayes was an audit partner in the Financial Services Practice of Ernst and Young.

Lehman Brothers

Lehman Brothers is a leading global investment bank, serving the financial needs of corporations, governments and municipalities, institutional clients, and high-net-worth individuals worldwide. Founded in 1850, Lehman Brothers maintains leadership positions in equity and fixed income sales, trading and research, investment banking, private equity and private client services. The firm is headquartered in New York, London and Tokyo and operates through a network of offices around the world.

The greatest business risk of all is the sudden loss of the ability to run your business at all. In recent years there have been catastrophic events, like September 11, which brought some businesses to a complete halt. There have been worries of catastrophic events, such as Y2K, the millennium bug, which failed to materialise. But the threat is always out there. The issue of managing business interruption is one of the hardest to deal with because it offers greater uncertainty and the possibility of greater catastrophic loss than any other business risk.

Some of the businesses which would have the most exposure to such situations are the global financial institutions with their second by second client dealings in the capital markets. Kevin Hayes would agree. He is a managing director of Lehman Brothers and its international chief financial officer. For him the issue of greatest importance is 'constant connectivity with our clients. It is fundamental to our business strategy. Clients have to have certainty that they have access to the markets through us'.

Communications are key and, of course, it is communications which are most at risk if the business or its environment suffers a catastrophic interruption.

For a business like Lehman Brothers the events of September 11 were the greatest test. No business can prepare itself for anything like that previously unimaginable disaster. But they had prepared themselves, through business continuity planning (BCP), for elements of it. 'September 11 is obviously in people's minds when they think of business continuity planning', said Hayes. 'It is a real life tragedy and a scenario of what can happen. It jolts everyone into thinking what the real risk issues are.'

Lehman Brothers, like everyone else, had never imagined something as immense and as horrific as that could happen. But the steps the bank had taken stood it in good stead. 'Our experience is illustrative', he said. 'You can only imagine the disruption caused by having the majority of our US-based producers displaced from our

headquarters. However, we recovered very quickly – even on September 11 we were able to provide funding to others in the industry to ensure that the markets continued to operate. It was because of the measures we had in place, and others we improvised, that we were able to maintain connectivity to clients and were fully operational when the markets reopened.'

A culture of Business Continuity Planning (BCP)

Post-September 11 regulators and industry groups have been very active in developing resources and standards to help business develop BCPs. The Financial Services Authority in the UK has published some excellent material on their web site to assist financial services companies. In addition, there are a number of consulting firms who can assist in establishing and training personnel in BCP. What is interesting are the lessons learned from events such as Y2K and September 11 and how they have shaped our thinking about BCP.

Historically, BCP was about data recovery. 'Has everything been backed up and do we have a remote location to continue business if the primary site is not operational? Today, it is now recognised that there is a need to integrate BCP into every business process', Hayes said. BCP is focused on keeping the critical element of the business process working in all circumstances as seamlessly and with as little externally visible disruption as possible.

One of the catalysts for much of the change in attitude has been the past work on the perceived threats of Y2K and of a millennium bug at the turn of the century. The whole Y2K period is now often dismissed as a bit of an embarrassment. Everyone spent a fortune, held their breath, and nothing appeared to happen. But what is now clear is that it changed attitudes and planning procedures for BCP.

'Businesses have been greatly helped by the Y2K process', said Hayes. 'In preparation for Y2K people thought more broadly about the possibility of threats, like sabotage, and considered the interdependence between their business and their suppliers and customers. Y2K was also a catalyst to update technology and systems applications to more current technology and to install redundancy in hardware and uninterrupted power supply' said Hayes. 'These processes have continued, and now they have been built in BCP'.

Home alone

It is a reality today that most people have computers in their homes and have access to the internet. Many of your employees may have a full home office set up. This can provide you with a practical opportunity in your BCP to augment other dedicated alternative facilities you have available. Even in a more humble break in continuity, like a transport strike, people can simply switch locations. In the aftermath of September 11 the finance department of Lehman Brothers became very adaptable. 'For a period half of our people were working from home', he said. 'We were able to expand our remote access technology to allow our employees to access applications and files remotely from home. It was not exactly part of the plan but it shows that in a crisis adaptability is a key to continuity.'

There is also an important human element that should be considered here. After an event, it is human nature for everyone to want to be involved in the recovery. It is however a matter of priority which business activities are recovered and when. It will therefore be necessary to classify some business processes and the associated staff as 'essential' and some as 'non essential'. For those 'non essential' employees it is vital for their morale to still feel part of the firm's activities. Our experience after September 11 said Hayes, was that it was essential to maintain morale through regular communication between those that were at work and those working from home or on furlough. This ensured that people felt connected and aided in their transition back to work.'

Connectivity

In any client-facing business the most important issue is client connectivity and therefore communication (telephonic and data lines) are essential. Again, on a tactical level, the majority of people have cell phones and this can provide an immediate solution. However, this is not a sustainable approach, a stable communication platform needs to be secured, clients must have the confidence that they can reach you to transact. 'Securing sufficient telephone and data line capacity is a vital part of a BCP, as well as establishing a plan of how to notify customers of new telephone numbers and connection points as contact numbers may change', said Hayes.

Hayes returned to the lessons of September 11. 'In a widespread disaster there are obviously issues of employee safety', he said, 'telephone-based systems are available to allow employees to call in and log that they are safe and where they can be reached. This is essential to be able to mobilise your work force after an event. Employees should know exactly who to contact, how to log where they are and how they can be contacted.

When the lights go out

A key element of a plan's success is rehearsal. How an organisation reacts in a crisis is more about its management culture and how different parts of the business co-operate together. These are things that a BCP cannot determine. A BCP can, however, provide a framework to add certainty in how to bring people together to operate in a crisis.

In any incident, information about what has happened is essential in order for management to make decisions. Establishing this communication can be problematic – the natural reaction of those immediately affected is to try to fix the problem and mitigate the risk. The BCP should force channels of communication to be established immediately and simultaneously by empowering personnel to declare a BCP event and start the recovery process. This will ensure that management has information on which to make decisions to mitigate risks both upstream and downstream of the event.

Location, location, location

Post-September 11, 'Companies have re-evaluated their occupancy strategies between being located on a central campus of related buildings, or having them distributed in separate locations', said Hayes. In all these decisions there are practical consideration but other less tangible issues can influence the outcome. 'Culture plays its part', said Hayes 'It may appear to be safer to move business units apart, but this can harm their connectivity'.

Consider those around you

Another related consideration is the location of essential suppliers and customers. The localised effects of September 11 impacted a group of related business in the financial services sector, including the organisation involved in clearing and settling securities between the various banks. Businesses should, therefore, not only evaluate their own situations but that of the businesses around them. This also applies more broadly to the state of preparedness of suppliers that are essential to the operation of your business.

Business disruptions can have a very unsettling effect on the business community that interacts with your company. The likelihood of business failure is very real. 'September 11 was felt all around the world', said Hayes. 'It was a catastrophic event, most threats however are likely to have a more localised effect (for example

power outages, weather related events, or a computer virus) . In these situations it is even more important to maintain contact with suppliers, lenders, regulators and customers, to ensure they understand what has happened and your progress towards recovery.'

Business continuity planning is designed to ensure that your business continues. A clearly thought-out plan covering the critical business activities, analysis of potential threats and actions steps to mitigate those threats are key elements of the plan. However, planning is only part of the solution. Rehearsals and debriefings are essential to build a 'recovery culture' so that personnel work collectively in those situations that are unplanned and unanticipated.

Risk Management

Reputational Risk

An interview with *Steve Marshall FCMA, former Group Chief Executive Officer, Railtrack*

Steve Marshall was group chief executive of Railtrack from November 2000 until March 2002, having joined Railtrack as group finance director in December 1999. Steve was previously group chief executive of Thorn plc, the international retail group, having joined them in 1995 as group finance and commercial director. He is currently a special adviser to CIMA.

Railtrack

Railtrack, formed after British Rail was privatised in 1996, owns the UK rail infrastructure and employs nearly 12,000 people. It is also one of the country's largest commercial property owners (managing some 22 million square feet of business space). Most of its revenue comes from fees paid by the country's 25 regional passenger-train companies and freight operators and public subsidy.

Railtrack Group has recently sold its operating subsidiary to Network Rail, a government funded vehicle. It has re-listed its shares and will return some £1.3 bn of cash to its shareholders.

A variety of stakeholders and reputations

At its lowest ebb Railtrack, as its then chief executive, Steve Marshall, will tell you, was 'in the top three daily television news items for 45 consecutive days'. It is small wonder that he has a tale to tell of how to manage reputation risk at the sharp end. And he also has a series of lessons learned which would stand any risk manager in good stead.

Marshall stepped up from his post of finance director to become CEO of Railtrack Group in November 2000, three weeks after the Hatfield rail crash had shocked the nation, and he remained at the post until March 2002. He tendered his resignation in October 2001 in protest when the then Transport Secretary, Stephen Byers, pushed the group's operating subsidiary into administration in the hope that it could be painlessly brought back into public ownership.

Marshall starts with the basics. Organisations like Railtrack are complex. 'When you are assessing your reputation and its risk you have to remember that there isn't just the one reputation', he said. The management of the reputation risk has to take into account all of the organisation's stakeholders. There can be many of them and they will all have different agendas and all will have a subtly different view of the organisation. 'Railtrack was unique in that it had an absolute constellation of stakeholders', he said. 'It had stakeholder overload'.

'First you had the general travelling public', he said. 'Then you had the Government and all its different arms, No 10 Downing Street, the Department of Transport, the Treasury and the civil servants. Then you had several regulators and the Health and Safety Executive. Then you had all the passenger interest lobby groups and then

the bereaved relatives'. Marshall draws breath. 'And then you had the bankers and the shareholders and all the stakeholders a normal company would have, not least your employees and contractors'.

All of these stakeholder interests had different needs, different perspectives and, in Marshall's words, 'different criteria for judging you'.

That sets the scene. But before he goes into the detail of how to handle all of those potential risks Marshall steps back to make one fundamental point which will colour all of his advice on risk management. He thinks that there is one abiding truth in the field of managing reputational risk that stands above all others. If this is understood then the rest have a more logical flow.

The fundamental truth and managing the business in the midst of crisis

'The fundamental truth which you only discover when you have gone through the fires of hell', he said, 'is that your reputation will always mirror the absolute reality of who you are'. This has enormous implications. 'Anyone who thinks that they can change their reputation without changing the company is mistaken', he said. Spin, in other words, can never change a reputation and can help damage it. 'Never think about the press release first', he said with some feeling, 'that is what governments do'.

Marshall talked frankly about how to deal with the sort of cataclysmic disasters which befell Railtrack at the time of Hatfield crash. 'How you deal with it depends on what situation you are in', he said. 'When you have a terrible disaster like Hatfield you start with a massive reputational deficit'. This is the point about being one of the main items on the main television news every night for a month and a half. 'You are constantly on the nation's radar screen', he said. 'It is a stunning reputational hit'.

Again he has one fundamental piece of advice. 'The first thing you have to do', he said, 'is to talk straight and tell the truth as soon as you know it. If you don't do that then you have nowhere to go'. The second piece of advice follows directly on from that: 'We tried very hard to show humility and to take responsibility'.

Then it is a question of being as direct as you can be with stakeholders. 'We spent a huge amount of time talking to all of our stakeholders from the bereaved families to Tony Blair', he said. 'An unbelievable amount of time was put into simply informing people of what was going on. The news was not good but they heard it from us and they heard it straight'.

Although no one could plan or predict what was going to happen in the ensuing months, Marshall did discover a silver lining, a benefit which derived from this policy. It came about when the huge row developed with the then Transport Minister Stephen Byers over financing and then over his plans to put the company into administration. 'When we went head-to-head with Byers the media did see us as open and straight', he said, 'and it is a formidable thing doing battle with a Government media machine'.

There is a key point here. 'You can build up credibility if you are open and straight', he said. 'It won't get you out of the hole. But on the margins it will make a difference. It will get you a hearing'.

The other point Marshall emphasised was how important it is to not allow crisis management to take your eyes off the real business issues. 'Never allow all this to undermine your work', he said. 'We had the network to look after, our financial obligations and our negotiations with Government for financial breathing space. You need to work on the reputation and build the credibility but the priority is to crack the underlying problems'. One part of this was to split teams between what Marshall refers as 'the day job' and the risk management efforts.

‘For example, the finance director took an increased part in the day job while several others and myself as CEO were much more into war council mode’, he said.

That is all the work dealing with the management of reputation risk outside of the business. Internal communications are just as important. Internal morale in particular is just as important as external viewpoints and the one can influence the other. ‘The most deadly sign of a reputation in trouble is when staff admitted to covering up their papers while on a train because they don’t want people to see that they work for Railtrack’, he said.

‘Staff are the most powerful ambassadors you can have’, he said. ‘I know it sounds like a management cliché’, he said. ‘but they are’. Marshall’s training was in accounting. He knows the power of numbers. ‘There are about 100,000 people involved in working on the railways’, he said. ‘If they talk to thirty or so people in the course of a month then that is getting on for upwards of three to four million people. That represents 10 per cent of the national adult labour force’. If honest and positive views are being expressed rather than the pessimistic tones of a workforce whose morale has gone then it can make a huge difference. ‘It does have a powerful effect potentially in both directions”, he said.

So it is an important part of your strategy to get out and about and talk to the workforce. ‘We did a lot of getting around the country and having face-to-face meetings’, he said. ‘During one three-week period, I met over 10 per cent of the workforce face-to-face to let people ask any questions they wanted’.

Marshall is convinced that this sort of direct communication is what pays off. ‘They can read in your face whether the company is going to make progress’, he said. ‘It makes a tremendous difference if people can stare into your eyes’.

Adding to this method of direct dealing with the workforce and backing it up are the other means of trying build anew in times of trouble. The press office needs to continually rebut what is being said about the company, for example. This gives the company something to build on. ‘Then’, said Marshall, ‘you pick up the phone to the other stakeholders’.

There were terrible times along the way. ‘We had some very dark moments’, he said, ‘and they were not the being dragged into Downing Street or being grilled by the media. It was the bereaved families’, he said. ‘No one can train you for that. Here were decent ordinary people who didn’t deserve to be in that situation. You felt desperately responsible’, he said.

Lessons learned

The Railtrack experience has provided Marshall with a series of lessons learned. But they are not the simple and practical things that you might expect. ‘None of the things that I learned were in the predictable areas’, he said, ‘like, for example, a strong press office which we had’. Instead what Marshall would put forward as the key issues in reputation risk management are rather deeper than that.

For him the key is more to do with scanning the horizon than dealing with crises. ‘It’s the fundamental understanding of how business risk arises’, he said. ‘Railtrack wasn’t on top of its game in its fundamental business understanding of the job. Prior to Hatfield there was no engineering director on the board, for example, and this in a business which is dominated by engineering. I appointed one on my second day in charge’.

There were other, almost inexplicable, aberrations. 'Railtrack didn't have a grip on its contractors', he said, 'and from that stems catastrophic business risk. It destroyed the brand's integrity'.

Marshall draws a series of simple rules from this. 'Have all the key areas of expertise at the top table', he said, 'and never lose sight of the fundamentals on a road to a growth story. It will betray you every time'.

He went back to his earlier observation about truth. 'You have to be authentic', he said. 'The company has to more than passingly resemble what you are saying that it is and all of senior management have to be authentic as well'. He drew a conclusion from this which would surprise many a CEO. 'Although I probably need it, I have always refused media training', he said. 'I have always been deeply suspicious that it would separate the product you are portraying from yourself'. He sees this as a real risk. 'Railtrack was not as good as it needed to be – so we had to admit that', he said.

Risk management also requires formal systems. 'It is how you put the mechanisms in place to ensure that these risks are being addressed', he said. 'The Turnbull guidance helps but it doesn't force you into the rigour of having a strategy for each of your stakeholders and how you get feedback from them', he said. 'You need to invest in reputation maintenance'. Looking back at the Railtrack experience he thinks that the company could have been 'more deliberate in managing those risks with our stakeholders'.

Another lesson learned was to build long-term relations with the media. 'We learned rather late in the day that because the media is so powerful it is important to build a long-term relationship', he said. 'Authenticity comes into it. It's a long-term build and it takes time'. But, as Marshall found during the last battle with Stephen Byers over putting the company into administration, it paid off. 'It worked in our favour over Byers', he said. 'The media held him accountable, which Parliament didn't'. Railtrack was by way of contrast voted 'Best Media Communicator 2002' by twenty top City editors – not bad for Britain's 'most hated' company.

The last of the lessons that Marshall would point to is one which is impossible to put into action. 'Don't be unlucky', he said. He argued that the way that Railtrack was put together made it the unluckiest company ever designed. 'First it had the dreadful inheritance of the rushed Conservative privatisation', he said. 'Then, despite having a better safety record than its predecessor, it had three high profile crashes. There were the stunning financial consequences of the Hatfield crash and the legacy of a contract for the upgrading of the West Coast line at a fixed price negotiated before your time', he said.

It is also a question of always keeping abreast of changing attitudes. 'The reactions of your different stakeholders change', he said. 'Public tolerance of a rail crash, quite rightly, is now much lower than it was twenty or thirty years ago. The frequency of crashes has not increased. It is the tolerance that has reduced'. Risk managers have to assess not just the reputation risk but how it changes over time.

In a situation like Railtrack it is a well nigh impossible task. 'It is very difficult', said Marshall, 'to have a privately-funded and stock market-rated company operating with government funding in a key public service. It is', he said, 'the hybrid from hell'. It is not so much a Third Way. For Marshall it was '"a blurred way" where everyone is dabbling and no one knows where the funding is'. And this was his final point on reputational risk. 'If you haven't got clear control and you have great complexity', he said, 'then things will go terribly wrong, and your reputation with it'.

Risk Management

Brand and Reputation

A view from Microsoft

An interview with *Steve Harvey FCMA, Director of People, Profit and Culture, Microsoft*

Microsoft

Microsoft is the world's leading software provider, offering goods and services as diverse as Windows Operating System and Office software to video games consoles, Internet access or interactive television.

Its 2002 sales were in excess of $28 billion. The chairman Bill Gates still owns 12 per cent of the company. So large are its cash flows (around $1 billion a month) that even in these difficult times for the IT industry it is able to increase R&D spend by 20 per cent.

External branding and internal values

Microsoft is different to other companies. It vies with General Electric for the title of having the largest market capitalisation in the world. It is the pre-eminent name in software, services and internet technologies. But more than that it is a company which has changed the way that the world works. It has done this by being different.

So it comes as no surprise to find that Steve Harvey is far from being a conventional finance director. For a start he is not a finance director, though he has held that responsibility for the last seven years. His official title, apart from deputising for the UK managing director, is group director of people, profit and culture. In another company you would simply say that the finance director has also taken over the human resources role, which he did five years ago. But that is not how they see it at Microsoft and that is why they are different. The company is trying to see everything differently and thereby create a competitive advantage. So the concept of brand and reputation risk is forefront in the company's mind.

The first principle Harvey seeks to establish is a simple one, but one which is often underestimated by other companies. 'What is important', he said, 'is that the external brand of the company is affected by internal values'. So at Microsoft Harvey tries to connect the two. 'Software is at the centre of everything we do', he said. The philosophy of the world-wide web connects seamlessly with employee policy. 'With our software we are empowering people to reach their full potential so we are trying to get the message through to the people in Microsoft that the job is not just selling software'. It is a view of the company and its relationship with society in general which is very different to that of most companies. 'Our software changes and helps people reach their potential', he said. 'That gives us a wider role'.

So internal values are very important to protect both brand and reputation. 'Hence', said Harvey, 'the word "culture" in my title'. There is a very simple equation at work here. 'We have to continue to find good people', he said, 'but they also need to be great employees. If we don't get it right then we won't get the longer-term growth or our long-term profits'.

In some ways Microsoft has to be different. It has some 50,000 employees worldwide but, as Harvey pointed out, some 20,000 of these are developing software. '"Creating the environment where great people can do their

best work" is the mantra for the people vision at Microsoft UK', he said. 'There are three distinct strategies that support this vision and help retain our top talent and with them we aim to address the physical, emotional and intellectual needs of our employees'. These three issues form the core. 'On the intellectual side', said Harvey, 'it is a question of allowing bright people to challenge each other and the business in productive ways. On the physical side it is a question of creating a physical space that enables our employees to do their best work and on the emotional side it is a question of establishing a well-being centre and providing day-to-day support'.

This latter meant the creation of programmes with names like 'fit for life' and 'personal excellence'. 'We introduced the benefits of meditation, good eating, how to rest and get recovery time, as well as the fundamentals of good time management', said Harvey.

A culture of financial prudence

For many hard-nosed managers this sort of programme simply means that the company has lost sight of the main issues. Harvey argues that this is not the case. The financials are still the key to the company. 'We are one of the most prudent companies you could find', he said. 'We have no debt. We have lots of cash and very few physical assets'. He cited the presentation which John Connors, the company's global chief financial officer, made at the company's annual conference in the summer. In the shadow of Enron, WorldCom and other great American corporate collapses the risk to Microsoft's reputation and brand was uppermost in peoples' minds. Reassurance was what was required. 'Connor's message was that there are no skeletons on our closet and that employees have nothing to fear', said Harvey.

He suggested that the culture of financial prudence went back to the company's beginnings. 'It goes back to the start', he said. 'Microsoft almost went broke in its first year. We never want to experience that again'.

So there is a strong connection between employee policies and financial objectives, which explains the make-up of responsibilities in Harvey's job title. 'All we have is people', he said. 'We look after them very well but everything we do has a business reason for doing it'.

Engaged employees

This leads to the philosophy of 'employee satisfaction versus engaged employees'. 'Employee satisfaction is a strange expression', said Harvey. 'Is it really possible to satisfy all employees? Pay rises are usually taken for granted within a few months and fringe benefits are usually too peripheral to making a significant impact on employee performance'. So Harvey changed tack. 'Microsoft has shifted the emphasis from employee satisfaction to focusing on employee engagement', he said. 'Microsoft is lucky to be able to hire many bright and talented people who have an unparalleled passion for technology and its role in changing the way that people learn, work and play. What is most important though is to ensure that an employee's passion for technology and the company's strategy are appropriately aligned'. It is a simple objective. People thrive in an environment where they are supremely involved and happy with what they are doing. If anything, it is startling how many companies and organisations do not understand this simple truth.

'As an accountant', said Harvey, 'you are always sweating your assets but people are your biggest asset. If you get the people side right then your long-term growth is assured. We have the highest revenue per employee in Microsoft worldwide'. And there is also the future to be factored in. 'In the future there will not be enough bright people to go around.', he said. 'We need them now'. This creates a very different attitude. 'We have a belief in creating a strength-based culture', Harvey said. 'We focus on what people are good at. Other methods,

like 360 degree programmes, go for the well-rounded focus. We are completely different'. Harvey has a very different view. 'People like doing what they do best and that is what makes them want to be here every day'.

This does not mean that the company goes soft. 'It is', said Harvey, 'people with an edge to it. It is not the fluffy sale. We need people as willing volunteers'. So the financial side has an edge too. 'People are always under pressure and tension to achieve goals and targets', he said. 'That's the mentality within. There is a hunger and a desire to do better'.

It also means a different approach to remuneration. 'Everything is done with good business in mind', he said. 'We pay people in stock. What matters is the long-term strategy. We pay at two-thirds of the market rate and give them stock. So it is in their real interest to raise the stock price'. You might have thought that this would put Microsoft at a disadvantage in the recruitment market. Harvey puts his HR hat on. 'The average length of service is seven years for senior people', he said, 'and three-and-a-half years for all staff'. And when it comes to top-performing employees, the people Microsoft calls 'A-raters', the company claims to have not lost one of them in the last three years.

'This is particularly significant', said Harvey, 'considering the massive drops in the company share price, the dot-com boom, and the best efforts of external head-hunters to lure our top talent away from the company. Microsoft UK currently boasts an attrition rate of just 2 per cent compared to the industry average of 19 per cent'.

Altruism as a corporate value

There is a strong message of altruism within the company. The internal view of Microsoft helping people to maximise their potential extends outwards. 'Our role is helping society', said Harvey. And that extends to other programmes as well. 'We do a lot of work in the community', he said, 'charity, children and education. We need to share our intellect, to help governments and communities and help our corporate social responsibility programmes'.

Harvey laid great emphasis on the corporate social responsibility side. The importance is that employees are involved. It is not simply a chunk of corporate money given away. 'There are lots of events which commit our employees', said Harvey, 'for example, we match both charity money raised and match the time involved'. The main beneficiary is the UK NSPCC, the national society for the prevention of cruelty to children, and Help The Aged.

Harvey provided a personal example. 'I run my own golf charity day', he said. 'I've raised £250,000 in four years now'. But, as you might expect the altruism is linked. 'So employees are engaged in that', he said. 'It allows us to be more connected to our customer base. We are out and about with both our business partners and our customers'. He gave the example of the Commonwealth Games in Manchester this year. 'It was the first event like that to run entirely on Microsoft systems', he said. 'It was a great learning experience for us and a way to give something back. And as a result the software gets better'.

This leads Harvey to another conclusion which once again reveals how different the view within Microsoft is. 'We make money as a by-product of being a great software company', he said. 'There is a very healthy tension between growing the business long-term and satisfying customers' needs every day'.

The prudence on the financial side extends through to the more obvious management of risk. 'We self-insure', he said, 'and we globalise risk wherever we can. We insure cars globally, for example'. This policy, combined with that of helping the well-being of the workforce, pays dividends. 'We self-insure on healthcare', he said. 'But we have a very healthy workforce and that has saved us a ton of money in recent years'. The treasury

function is carried out through the US. Harvey emphasised the care again. 'We are very prudent with our own financials', he said. 'We don't defer costs. We are lucky in having run the company prudently', he said. 'We have to ensure our house is clean and in order'.

Reputation, brand and risk management

The biggest risk to Microsoft is, of course on the reputation side. 'The biggest risk is if the products don't produce', as Harvey put it. Here again they put their faith in connecting with customers. 'The system is geared around helplines', he said. 'We actively capture feedback. Software updates happen automatically'.

A company like Microsoft and in Microsoft's position is, in many ways, unique. But it has its priorities right when it comes to reputation and brand risk. 'There is a lot of positive noise around how Microsoft has run its people strategies', said Harvey. 'It is a very effective and efficient corporation'.

Risk Management

Risk in the Acquisition Process

Bill Connell FCMA,
Director of Risk Management, BOC Group

Bill Connell is Director of Risk Management, BOC Group and Chairman of IFAC's Financial and Management Accounting Committee. With the emphasis on acquisitions as part of its strategy, it is necessary for BOC to understand the risks in the process.

Mergers and acquisitions are notoriously risky and often fail to deliver the benefits envisaged when they are approved. They can be driven by emotion and enthusiasm rather than fact and logic, and are frequently poorly managed. This article, therefore, attempts to identify key issues and put forward an approach whereby risk plays an important role in the acquisition process. The sections are:

1. Why acquisitions are different
2. The acquisition process
3. The role of risk management in acquisitions
4. Summary

This article is based on case studies in the BOC Group plc (an industrial gases and vacuum company that operates in over 50 countries) and on research on best practice in acquisitions.

1. Why acquisitions are different

A KPMG survey in 2001 of acquisitions revealed the following statistics:

- 30 per cent of deals added value;
- 39 per cent of deals produced no difference;
- 31 per cent of deals destroyed value.

The common reason for failure was a lack of effective project management and the research indicated that companies adopting effective project management were 29 per cent more likely to be successful than those without.

A quote in the *Economist* article 'Why too many mergers miss the mark' commented:

'What does seem to link most mergers that fail is the acquirer's obsession with the deal itself, coupled with too little attention to what happens next – particularly the complex business of blending all the systems, informal processes and cultures that make the merging firms tick.'

Research by Ernst & Young indicated that internal issues were cited by 58 per cent of respondents as the main reason why cross-border acquisitions were riskier than domestic ones. This seems to indicate that such things as regulatory differences and differences in standards are considered to be surmountable, but that most intangible differences, such as cultural ones, are more difficult to crack.

Further quotes on integration highlight the issue that post acquisition is always the last piece attended to:

'Planning is the exception, not the rule, and a large number of acquisitions fail because companies do not plan integration as part of the deal.'

'Most top executives are aware that poorly conceived or overpriced acquisitions are doomed to failure regardless of subsequent events, but few appreciate that even well-conceived deals can quickly disintegrate without active and sharply focused management of the post-acquisition integration process.'

I J.R. Harbison and *S.J. Silver*
Booz-Allen & Hamilton

'The weak spot in the acquisition is right after the deal is completed. That is when companies face value-killing indecision and aimlessness.'

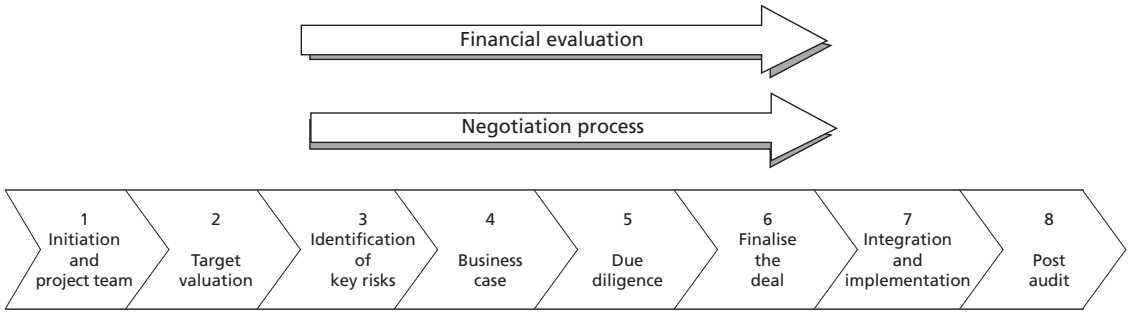
Mergers and Acquisitions Magazine

2. The acquisition process

Like many aspects of business, the need for acquisitions must come out of a good (and agreed) strategy process and should be the result of target spotting. Rarely do successful acquisitions come out of opportunistic approaches by buyers or sellers where it is then rationalised as a strategic fit.

The process map below, therefore, starts when the target has been identified and is regarded as a strategic fit. Arguments are often made that the sequential steps in the process are not reasonable when the pressures of financial evaluation and particularly re-negotiation are layered on top. In effect these two processes can go through many interactions during steps 2 to 6. In some instances, some of the steps will be run in parallel.

The key stages in acquisitions from a BOC approval perspective



There are three key stages in the process that ensure a successful process:

Phase 1 – setting up

This occurs at the very earliest stage and should ensure that the right resource is allocated to the project covering both in-house and external resources. Companies who had an experienced process/project manager in acquisitions from target identification until post implementation evaluation were 71 per cent more likely to be successful than those who did not.

Phase 2 – business case

This occurs as Stage 4 and should articulate the rationale for the acquisition, the financial evaluation including confirming early assessments on synergies, the key risks, and should outline the key activities that need to be carried out to better manage the acquisition process.

Phase 3 – finalise the deal

This occurs as Stage 6 and the critical steps here are to ensure that:

- due diligence has been properly carried out and that there are no issues;
- the deal reflects the business case;
- there is a clear integration plan.

BOC has now formalised the process for each step and the complete process and the CEO has sent a note out to all businesses mandating its use of the process. The Investment Committee tracks all acquisitions from early warning papers to post audit and reports on the steps for each in a monthly summary. Research identified that:

- Transactions are more successful in creating shareholder value where clear decisions are taken about how each of the steps will be managed and by whom.
- Successful acquirers (remember the low success rate of 30 per cent) undertook all stages earlier in the process than those who failed to create value.
- Companies who failed to create shareholder value in acquisitions responded that they would have undertaken all activities earlier if given the opportunity to re-perform the transaction.
- Adopting a thorough process with clear responsibilities increases the likelihood of success by 29 per cent.

3. The role of risk management in acquisitions

Risks in acquisition

There are many risks in an acquisition, as already identified earlier in this article. It is critical to manage all of the risks at the earliest stage possible. The fundamental questions to be asked are ***Why are we buying?*** and ***Why are they selling?*** Answers to these, well articulated, are early indicators of a successful deal. Conversely, gaps in the answers often highlight the key risks that will face the acquisition.

Output from the bid preparation will define the risk management process:

- Is the deal consistent with the business strategy?
  - — access to geographic/sector markets;
  - — market leadership positions;
  - — manufacturing overlap/product sources.
- What is the quality of the business being acquired?
- What is the track record of the acquiring management team?
- Has the management team considered alternatives to acquisition? (e.g. internal development or alliance/partnership).
- Does the management have the capacity to integrate the deal?
- At a high level, what are the synergies available?

- Can the deal be financed?
  - How?
  - How does this impact other cash needs?
- What is the quality and motivation of the management team being acquired?
- Early identification of potential deal breakers?
- Fix the maximum you are prepared to pay and walk away – don't get sucked in.
- Evaluate all ways of getting an inside track to get priority bid status.
- Identify the other potential bidders and undertake a competitive bid assessment.
- Don't lock yourself in or over-commit in the initial bid.
- Have a clearly defined negotiation strategy for the next phase.

Risk management process

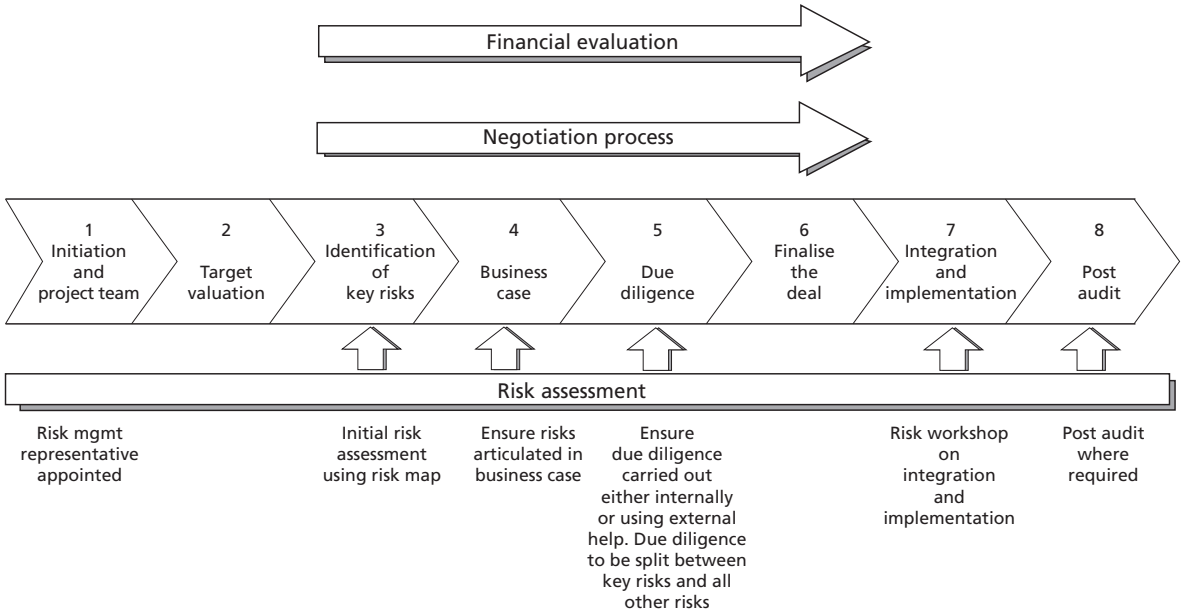
Project management must pick up the risk management process. This is often facilitated by an expert (i.e. risk specialist) and this is expanded upon in the next section. A list of the tasks for risk management includes:

- Repeatedly check the strategic and business rationale as new information is disclosed.
- Perform external checks on the target's management team.
- Compile a checklist of 'doomsday scenarios' and ensure all have been assessed.
- Ensure the deal team is balanced: internal deal practitioners; external advisers; management responsible for subsequent performance etc.
- Take the synergy plan to a high level of detail, include costs and timings, get both managements to commit to the targets if possible.
- Plan the integration in meticulous detail, including resourcing.
- Understand all political, regulatory and environmental risks.
- Have a clear set of actions on day one and in the first few weeks.
- Decide early on the composition of the new management team.
- Have a clear communication plan for all stakeholders.
- Anticipate potential employee issues, particularly where unions or works councils are involved and redundancies are planned.
  - How could they disrupt the business?
- Understand the IT systems in detail and how they will be integrated. Make sure a very strong technical service agreement is in place if necessary, with appropriate regular service delivery assessments.
- Keep an eye on spoiling tactics by competitors.
- Negotiate the sale and purchase agreement (SPA) to allow for price adjustment.
- Check for change of control clause – everywhere.
- Ensure target management are locked in where desired and that mechanisms are in place to retain their motivation and hunger.
- Be prepared to walk away!
  - Objectivity is critical, especially approaching closing.

The risk management process in BOC

Given that an acquisition process was mandated in BOC, consideration was given as to how the risk management function could add value to the process. Due diligence is well recognised as a process for reviewing the risks in an acquisition, but it is often too late in the process and it would be more effective if risks were identified at the earliest possible stage and the potential show stopper risks prioritised.

The following diagram builds on the process map and identifies the responsibilities of a risk management function.



While full guidelines together with tools and techniques have been developed for each stage, the following gives a brief summary of these.

- *Stage 1 – Initiation and project team*
  Risk management representative appointed to the project with responsibility for ensuring risk management support is provided at each stage. This is likely to be different people at different stages to reflect the skill requirements, e.g. carrying out due diligence, facilitating an integration and implementation risk workshop or external specialists if necessary.

- *Stage 2 – Target valuation*
  This is the area for the corporate finance professional to assist in the acquisition process, but the techniques are not covered in this article.

- *Stage 3 – Identification of key risks*
  The use of a 'risk map' enables the risk specialist to conduct a discussion with the project manager – usually lasting two to three hours. The business risks need to be evaluated from all angles – strategic, financial and operational. The topics covered in the discussion are:

  — business environmental;
  — operational complexity;
  — financial health;
  — impact on BOC (i.e. acquirer);
  — future;

  and each heading has a list of sub-headings to promote discussion. The objective of the exercise is to identify the key risks relating to the specific acquisitions (normally around five) and to ensure that future work is focused around these key risks. This process also helps to prioritise due diligence and avoid the situation where key risk areas are poorly addressed by the target in any data room or due diligence exercise, whether intentional or not!

- *Stage 4 – Business case*
  To ensure that all the key risks are included in the business case. There is the temptation to say that a certain risk is 'out of scope' by the local project team where in fact it is a critical requirement in a corporate review.

- *Stage 5 – Due diligence*
  Full checklists are required for due diligence with the person responsible for carrying out the work and the manager responsible for signing off the opinion/result clearly identified for each of the items on the list.

  It is useful to bring in corporate or global business functional managers to sign off the important areas of due diligence which of course vary by acquisition but may, for example, be HR or safety related.

  A primary purpose of due diligence is to ensure that there are no 'black holes' in the acquisition. A recent survey identified that deals were 26 per cent more likely to be successful if acquirers focused on identifying and resolving cultural (or soft) issues in the due diligence process.

  On significant acquisitions, a full time due diligence co-ordinator is required who will manage this important process and produce weekly executive reports highlighting issues.

  This executive report on due diligence is an essential document in finalising the deal and may indeed be the main topic in a final review before completion.

- *Stage 6 – Finalise the deal*
  There is a need for a formal sign off before the deal is finalised. This can take the form of a 'sponsor's note' which provides a final summary of the key points – e.g. commitments, due diligence outcomes, warranties and indemnities, risks and mitigation, resolution of issues etc.

  Copies of the sale and purchase agreement and any other documents relevant to the transaction should be attached to the sponsor note.

  This process clarifies the basis of the final decision and ensures that all are aware of conditions and of course risks in the deal.

- *Stage 7 – Integration and implementation*
  Much of the loss on value in acquisitions occurs because of poor integration and implementation and yet this is an area poorly covered in acquisitions. The risk specialist can ensure that the risks at this stage are well understood and that appropriate mitigation plans are put in place. A workshop format has been developed to prioritise the key risks and ensure a successful integration. Best practice is to carry out this exercise as soon as possible after the deal is finalised. (Note that an integration plan is required at the business case – Stage 4).

  In the critical early stages of the acquisition successful integration will include early planning, swift completion of tasks and clear communication.

  The specific integration plans focus on integration of:

  — processes and functions (especially when impacting customers);.
  — technology;
  — people and culture.

Some best practice guidelines on integration and implementation:

Integration leadership

The complexity of integrated programme management requires a full time leader who focuses exclusively on directing the process.

Strategy alignment

Creating and disseminating a document that focuses the integration team on the acquisition value drivers ensures prioritisation of critical activities. Regularly requiring the integration leader to appraise the CFO and board of directors of progress against documented strategic integration activities mitigates the risk of task misprioritisation.

Employee communication

Building comprehensive communication plans that provide early, frequent and clear messages.

Key talent identification

Interviewing senior executives in the target company regarding key mid-level personnel and evaluating employees' performance on integration teams increases the probability of identifying 'hidden' talent, enabling the acquiring company to target and retain these valuable employees.

The final guideline on integration is: 'The first 100 days after acquisition are the most critical for success – the process is often derailed because of speed'.

The following is a typical, but not comprehensive, list of actions arising from a risk review.

- Rigorously maintain senior management focus on delivering the identified benefits.
- Make sure the Board is aware of and involved with the progress:
  - keep the pressure on.
- Make it clear the integration leader has full management and board authority.
- Take people decisions fast:
  - don't have leavers hanging around causing problems.
- Make sure team leader and integration resources are in place and where necessary full time allocated. Fast integration must be their number one priority.
- Initiate the communication plan, make sure all stakeholders are involved and check that messages are being received and understood.
- Visit all the key customers to retain their business.
- Control the chequebooks, capital authorisation and signing authority.
- Deal with unexpected issues fast:
  - don't let them multiply;
  - have an escalation process.
- Watch out for spoiling from inside your business:
  - some people may wish to see the deal fail, often for non-obvious reasons.
- Don't let the costs creep:
  - hold people accountable for plans and estimates.
- Pay special attention to IT, especially security against disaffected employees.

- *Stage 8 – Post audit*
  The audit function can assist in the post audit exercise with the focus on establishing learning.

  There should be a formal process for post audits – normally twelve months after the completion of the acquisition and, of course, to assess the results of the deal.

  As part of the learning, old and expensive mistakes can be eliminated to ensure that shareholder value is maximised.

  Surprisingly, in recent research it was stated that less than half (45 per cent) had carried out a formal post-deal review.

4. Summary

Given the poor results from acquisitions and the enormity of risks that arise both during the pre-bid, the due diligence and the post-bid activities, it is surprising that more focus has not been placed on acquisitions.

The research has identified the following as key requirements to ensure success:

- Effective and experienced project management is essential and a full time role.
- Rigorous evaluation of synergies and ruthless implementation of these is essential.
- Effective due diligence is critical.
- Experienced specialists are essential – who have recent deal experience. This is not a job for the inexperienced executive, even if he/she have been successful in other roles.
- Identify risks at the earliest stage possible and rigorously evaluate, mitigate and action.

Risk Management

Capital Structure Risk and Bond Rating Agencies

Raymond Darke MBA, FCMA

Raymond Darke is a veteran of the Canadian Financial Services Industry and currently Executive-in-Residence at the DeGroote School of Business McMaster University, Hamilton, Canada

In this context, capital structure includes the degree of financial leverage (gearing) consistent with the business risk of the enterprise. The decision here is the appropriate level of tax-deductible debt in the overall capital structure consistent with the volatility of operating income. Cost of capital declines as leverage is increased but probability of insolvency increases. Finding and managing the optimal point is a key contribution of the CFO or strategic financial professional to overall strategy. Associated structural decisions include the issuance of equity, hybrids, convertibles, and the use of derivatives, off-balance sheet structures and customer financing captive subsidiaries.

There are three main bond rating agencies designated as Nationally Recognised Statistical Rating Organisations (NRSROs) by the US regulatory authorities. These are, Moody's, Standard & Poors and Fitch, with the first two controlling about 80 per cent of the world-wide bond-rating business. In addition, there are national agencies operating in various countries such as Dominion Bond Rating Services (DBRS) in Canada. This structure is essentially a duopoly with Fitch tending to focus on European issues.

There has been much cynicism lately about the nature of financial models used by equity analysts to establish equity valuations and future prices. Bond rating agencies tend to be much more focused on free cash flow and future events, which will impact this measure. Furthermore, their methodologies will focus on fundamentals such as stability, industry market share (#1 wins, #2 makes it, #3 must have specific niches, #4 struggles), size, quality of management, and intensity of competition as used by DBRS. Generally, they are exempt from selective disclosure laws so there is the perception they have information otherwise not available. This may be so, if the company decides to provide such information.

The process of establishing a rating involves initial discussions, reviews of collateral, structure and legal issues culminating in a decision by the agency's credit committee as to the rating to be assigned, with an appeal process if necessary, and then on-going monitoring. Both initial and on-going costs are borne by the issuer.

The value of ratings, is, of course, that a favourable rating will mean lower spreads for the enterprise and a broadening of the potential investment pool. For securitisation strategies, the creation of different tranches for investors with different risk appetites requires a suitable rating for each tranche. Agencies essentially have two roles, signalling and certification. Signalling implies of course new information. A strong signal would be a downgrade of the corporation's issues. If the downgrade lowers the enterprise's debt issues to below 'investment grade', this has serious consequences since many institutional investors are prohibited from investing in these issues, thus seriously depleting the potential investment pool. Interestingly, an academic study in this area suggests that bond rating downgrades are partially a response to information which markets already have. However, the perception is that this is new information, markets react negatively, and equity analysts revise their estimates sharply downwards. On the other hand, the market appears to believe that an upgrade provides no new information since there is usually no market response. As well, the astute CFO will also be interested in the bond market itself where bond prices provide real-time feedback of the assessment of the credit situation for individual companies.

More recently, rating agencies have come in for much criticism. On 20 March 2002, Senator Joe Lieberman, Chair of the U.S. Senate Committee on Government Affairs said in a statement, 'In the Enron case, I would have to conclude that the credit raters appear to have been no more knowledgeable about the company's problems than anyone else who was following its fortunes in the newspapers.' The statement further said that on 29 October 2001, Standard & Poors credit rating analyst appeared on CNN and said that 'despite Enron being on credit watch, Enron's ability to retain something like the rating that they're at today is excellent in the long term'. On 28 November 2001, both Moody's and Standard & Poor's downgraded Enron's issues to 'junk' status. These events and others suggest that the agencies may be now highly motivated to signal status changes as soon as possible. Moody's for example downgraded 172 companies, affecting $US 332.7 billion in debt in the second quarter of 2002. If this development is combined with any tendency for the agencies to not give specific rationales for changes in approach there are some serious implications for CFOs.

Essentially, if they have not already done so, senior finance professionals must become accustomed to operating in a 'goldfish bowl'. Company strategies are likely to be second-guessed, and negative assessments of future markets and strategies may be published unexpectedly. For example, this year DBRS published a report that states that projections about the potential size of the North American wireless market may be overly optimistic and that carriers needed to focus on profitability rather than subscriber growth. Presumably, if that were not your strategy, the agency would take a negative view.

There will be increased interest by the agencies in the internal audit function of companies, and pressure to release other requested information that the agencies consider to be part of a company's risk management process.

CFOs will need to be the custodian and guardian of a prudent financial approach as the rest of the executive team debate business strategies. For example, maintaining existing financial leverage as new projects are reviewed through the capital budgeting process.

A useful approach here is the 'sustainable growth equilibrium' expressed as: g=PRAT where g =growth, P= profitability, R= the retention ratio of earnings retained in the business, A= asset turnover, and T= leverage.

This deceptively simple relationship provides a way of focusing on the implications to leverage in reductions in profitability, margins and capital productivity and increases in earnings distribution.

They will need to be the champion of a cool assessment of the implications of major transactions such as mergers and acquisitions and make decisions such as whether to finance through equity or debt. CFOs will need to focus the debate on the net present value of synergies minus the premium paid for acquisitions as the basis for proceeding with the transaction. This equation seems to have been forgotten in the recent examples of over-payment for many acquisitions. They will need to speak against notions such as 'if it's a strategic acquisition, price doesn't matter'; or 'as long as we issue stock, valuation isn't that important.'

Other major transactions such as buying back equity by adding to debt, with the implication that management is better able than the market to value company stock, will need input. It sounds attractive to shift risk from equity to the debt-holders but if the decision results in no movement of the stock price, leverage will still remain. Finally, unexpected events, such as sovereign intervention (Argentina); counter party collapse (Enron); large adverse litigation judgments; etc., require worst-case scenario planning exercises in advance not *ex post facto*. Not the most popular role to play on the senior management team but nevertheless essential.

Additional suggestions from Standard & Poors for prudent pre-emptive actions include the following:

- avoid excessive, short-term, confidence-sensitive debt;
- stagger debt maturities;
- maintain cordial relations and credibility with banks during bad times and good;
- negotiate loose bank loan covenants while the company is financially strong;
- maintain bank lines in excess of anticipated needs;
- negotiate renewals well in advance of expiration;
- fully draw credit lines at the onset of major difficulties.

In summary, strategic financial professionals must anticipate unexpected negative events and plan for them, however unpopular that may make them. Transparency in financial statement preparation and investor relations is paramount and conservatism is the order of the day even in a bull market. Conservatism in decisions about capital structure and leverage both in the original strategy and management of ongoing operations. Conservatism in the assessment of major 'bet the farm' strategies. We may need to recall that equity, while capable of being leveraged is an essential buffer against unexpected negative developments.

Risk Management

Developing Risk Assessment in your Organisation

David Smith,
KPMG

David Smith is a member of KPMG's European Enterprise Risk Management practice and is based in London. He specialises in the design and implementation of enterprise risk management frameworks and methodologies – in particular the impact of risk on business strategy, organisational culture and intangible asset bases. David has over five years' risk management experience, working with a diverse range of organisations in a variety of industries, including logistics, consumer markets and financial services.

The tide of corporate governance regulation witnessed during the 1990s brought with it an increased need for organisations to better consolidate information on their key risks and escalate this information, in an understandable and digestible format, to the ultimate owners of risk – the board.

Citing compliance requirements as the key driver in the development of improved risk evaluation and reporting ignores the very practical, and for some, considerable business benefits of taking a more structured and business-relevant approach to the management of risk information. It has meant however, that most organisations have developed a form of 'risk register' or 'risk profile' generally updated through enterprise-wide risk assessments.

Presently many organisations are starting to question the real value delivered from such a compliance driven approach. As some within the field of risk management are developing methodologies for the detailed (financial) measurement of previously intangible forms of risk, other – more fundamental – questions remain unanswered, namely:

- How does the way in which an organisation captures and measures information on its key risks influence how effectively it manages those risks?
- What does current good practice look like? *and*
- How are organisations looking to develop their approach to drive more value from what for many remains an exercise in compliance?

Developing the risk profile

To respond to these questions it is necessary to revisit the foundations on which organisations have established their risk identification and assessment processes and the principles that inform them. Through doing so, it will hopefully become apparent that in making relatively minor adjustments to their processes for risk assessment, organisations can improve not only the effectiveness of these processes but the level of organisational awareness of, and ability to manage, their risk environment.

Assessment criteria

Fundamentally, if the process of escalating key risks is to be successful, the risks identified throughout the course of an enterprise-wide process of risk assessment need to be prioritised, and prioritised consistently, so that the most pertinent risks to strategic objectives rise to the top of the pile.

To do this most organisations have implemented rating criteria to assess the potential impact and likelihood of risks occurring. At its most crude the rating of impact takes the form of high, medium or low criteria. More developed and increasingly common approaches involve rating by approximated financial impact.

When establishing financial criteria for the impact of risk, many organisations fail to make the criteria relevant to all parts of their business and its operations. Initially this may not appear that important as, from a compliance perspective at least, the board only need to understand the impact of risk on their organisational financial objectives. But, as all well managed businesses cascade their financial objectives, it makes sense to cascade the criteria by which business operations assess the impact of their identified risks.

Where organisations decide to do this, some work will be needed to manage the practical consolidation of risk information and its escalation to board level. In our experience, however, this additional effort is easily outweighed by the increased relevance the rating of the risk has to those who are responsible for managing the risks on a day-to-day basis – the business operations themselves.

Additionally, limiting the categorisation of risk impact to purely financial terms ignores the wider, less tangible, impact that a risk may represent. The most pertinent of these impacts include the erosion of organisational reputation and the unforeseen drain of management time that results from fire-fighting or limiting a particular event's impact on the business in the long-term.

Risk categorisation

It is just as important for organisations to understand how to categorise the risks that have been identified as to evaluate and judge the potential impact of their risks. The classification of areas and types of risks establishes a consistent terminology for risk to be used across the organisation, and enables those responsible for analysing the risk environment to identify accumulations of risk across the business arising from a single event or cause. As very few risks impact their related processes or business objectives in isolation, an understanding of the interdependencies between them is essential to the appreciation of an organisation's true risk profile and its capacity or tolerance for risk at a strategic level.

Where risks are categorised by their origins in terms of operational structure, their nature or type of risk and, their relation to cross-organisational business processes such as selling, delivery, sourcing and facilities, decision-makers are better able to understand:

- Where risk resides in their business;
- How resources may need to be better targeted;
- How this may affect their development of strategy going forward.

Just as the cascading of criteria used for rating risk impact is essential in making the risk assessment relevant to operational management, the allocation of ownership for risk and accountability for any remedial or control actions identified during the assessment process, is essential in getting operational management to focus on their responsibilities for managing their risks.

Better aligning risk assessment with performance setting and monitoring

Increasingly organisations are focusing on how their ability to manage risk impacts business performance and their ability to achieve their objectives. Add to this the fact that with many risk assessment exercises taking the form of discrete processes that do not align with any form of business planning, many organisations encounter difficulties in engaging their management teams, and it becomes clear that developments need to be made in order to drive some real value from the measurement and monitoring of risk.

One very simple way to meet this development need is to improve the alignment of risk assessment activity with organisational business planning and target setting. As business planning in many organisations already requires that management identify the key risk factors to their operational performance targets, it makes little sense to carry out a risk identification and assessment exercise that is not connected to the objectives that management sign up to. Through incorporating the risk assessment process with business planning, management accountability for risk is visibly increased, with the risks identified used in the discussion between senior and operational management to challenge assumptions and set performance targets that are both stretching and achievable.

In addition to the development of an enterprise-wide appreciation of risk, the 1990s also witnessed the growth of organisational performance monitoring facilitated by the technology and communication innovation brought by the digital age. The use of key performance indicators (KPIs) and balanced scorecards is now well established as evidenced by a recent KPMG survey in which business leaders stated that measurement systems were very important for the achievement of their business objectives (*Achieving Measurement Performance Improvement in a Changing World: The Search for New Insight*, KPMG Assurance and Advisory Services Centre, New York, 2002).

With organisational risks also being assessed and monitored against the same objectives, it is a logical step to explore how these two activities can be combined. In order to achieve this, organisations need to understand both the critical success factors that contribute to the delivery of their objectives and the risks associated to them.

The technology question

As with organisational performance measurement and monitoring, technology certainly has a growing role in how organisations measure and monitor their risks. However, technology is by no means an answer in itself, and the execution of database systems to monitor risk profiles is often flawed when the basics of risk identification and assessment detailed earlier have been overlooked.

Risk management at the level of organisational risk identification and assessment is not an overly technical or scientific process. All too often the desire for the improved analysis and interpretation that technology can enable is unwittingly prioritised over the softer issues of management buy-in, risk ownership and accountability. Improving an organisation's appreciation of its risk environment and its ability to successfully manage the risks it encounters on a daily basis is in essence a change process, and technology alone will not deliver that change in isolation.

The way forward for your organisation

The effective measurement and monitoring of risk is central to the successful management of risk and delivery of organisational objectives. Yet through the course of our work we have found that a number of relatively

minor process improvements can dramatically improve both the quality and relevance of risk information received by the board, and how risk is regarded within the business.

Organisations that have been successful in these areas are now developing their risk assessment activity through improving its alignment with business planning and performance monitoring. Through understanding that the promotion of an improved appreciation of risk in their core managerial processes can lead to improved decision-making, these same organisations are deriving real organisational value from their risk assessment activity while at the same time meeting their compliance requirements.

Risk Management

An Internal Audit Best Practice Case Study

An interview with *James Duckworth FCMA, Chief Internal Auditor, Unilever*

In 1968 James Duckworth joined Unilever's internal audit department. His first assignment abroad came in 1973 when he worked for Lever y Asociados in Argentina for two years. Returning to the UK as commercial director, United Agricultural Merchants, he then held the post as chairman of Unilever Merseyside Ltd. In 1984 he moved to Kenya as Vice Chairman Unilever East Africa and chief executive of a joint venture between the World Bank, CDC and Unilever – the Oil Crop Development Scheme. From Kenya, James Duckworth moved to Unilever's head office in Rotterdam in 1987 as SVP Finance of Ice Cream Worldwide. In 1993 he was head of Information Technology for Unilever world-wide, a post he held for six years until 1999 when he became Chief Auditor.

Unilever

Unilever, owner of food, personal care and cleaning brands such as Birds Eye and Dove, is now the world's third biggest packaged consumer goods company. It employs nearly 300,000 people and its 2001 sales exceeded $50 billion.

The company has recently split into two global divisions, food and non-food, and plans to rationalise its huge portfolio of brands. Its two holding companies, Unilever Plc (UK) and Unilever N.V. (The Netherlands), have separate stock listings but share an identical board of directors with dual headquarters.

Bottom-up risk management

What James Duckworth, chief auditor at Unilever, is looking for is 'a canvas of unlimited scope'. His aim is to be as specific as he can in assessing and managing risk. But he also wants to ensure that nothing eludes the company. There are some basic principles underlying this approach. 'We look at the major risks', he said. 'But we increasingly take an attitude that the aim of an enterprise culture is to create change and be innovative'. And to achieve this another attitude needs to be nourished. 'We work in a spirit of "no limits"', he said. 'The auditors should not be restricted in any way in what they say or what they investigate. That gives us a canvas of unlimited scope'.

That might sound as though it is an undisciplined approach. This is not so. 'We are very selective in what we look at', said Duckworth. 'There is no use in having reports on a scatter-gun approach'. To achieve this selective but effective approach Unilever has to see the process as one running throughout its organisational hierarchy. 'We need to give major recommendations to the board which have been consistently researched through the group', he said.

This is the sort of approach which has revolutionised internal audit in recent years. The days when the function of an internal audit department was to say to itself that there were 500 units in the organisation to look at over the next five years and then to proceed to plod through the process are over.

There is also a much wider remit. 'We are talking about overall governance as well as corporate risk management', said Duckworth. The process has also been allowed to grow into a system which is, in part, giving responsibility further down the organisation. 'A huge part of the business is self-auditing', he said. 'People have to give a signed statement to the board of directors covering breaches of our code of business principles, compliance with policies and assurances on the accuracy of accounting and reporting procedures'. This process is then built on further. 'They then give an overall assessment in the form of a risk matrix of what they see as their top ten risks'. These are colour-coded as to degree of risk and go forward up the organisation.

Corporate risk committee

There are 300 operating companies which report through thirteen business groups to the corporate risk committee. This group of people is made up of the finance director, the human resources director, two divisional directors, the company secretary, controller and chief auditor. 'It is', as Duckworth said, 'a very powerful group. We consolidate the information and look at the overall top ten risks'.

The committee then adds its own thinking to the risk assessment. It overlays the risks put forward by the process with its own 'highest risks'. 'I put into these the risks that I think people won't admit to us', he said, 'for example, pressure on the accuracy of provisions. So I put it in as a major concern'.

This whole process gives Unilever a view based on risks which have been gathered in from three different directions.

Then the examination process takes place. This works in two ways. There are routine audits which check governance issues, breaches of the code of business principles and policy and accounting issues. Then there are audit reviews. 'There are four or five of these each year', said Duckworth, 'where we agree with the audit committee and the board that we will take a particular aspect apart, for example, it could be cash management'. In those cases they put a special team together and test the area out in depth and finally report through to the executive and audit committees.

A new culture for internal audit

Duckworth paid tribute to the culture of internal audit in Unilever. 'The good news is that Unilever's audit department has always been highly-rated'. He quotes a chairman from back in the 1960s as saying that: 'You ignore the advice of Audit at your peril'. This gives Duckworth a degree of assurance. 'I have no restrictions in what I can say', he said, 'which is a good feeling post-Enron'.

He feels that many organisations failed to recognise how the issues had changed. Looking back he sees that organisations were slow to realise how the world of risk management and internal audit had begun to alter significantly both in terms of objectives as well as the areas and types of risks involved. 'We had not recognised the fast changing pace of the world', he said. 'We were still focusing too much on the profit and loss account and the balance sheet and on fixed assets. They were important but those areas are not what kills businesses now'.

The whole focus has changed. 'Businesses now get killed off because of reputation risk', he said. 'They don't get killed off because the fixed assets are wrong'. He looks back a few years. 'The auditors were dinosaurs', he said.

'We have changed the approach to self-assessment', he said. 'If we find people have said something which is not true then this is a very serious matter and if what they have said is inaccurate then we investigate the process as well'.

The change of focus is total. 'I want my audit work not to show what happened in the past', he said, 'but to look at the issues ahead which may trip us up'. And the nature of the message which the process brings to the top of the organisation has changed as well. 'It has now translated into a message of: "You are going to need to do these things in the future"', he said.

All of this has been given a mighty shove by the disasters on the American corporate scene. 'The whole issue of Enron and the other scandals has increased people's awareness of audit and its responsibilities', he said. 'People will ask more questions'.

This, Duckworth thinks, will change the way people work. 'Now audit teams always need to be pressing managements', he said. 'Companies with the right attitude pre-Enron will still have the right attitude post-Enron', he said. 'For them it will be a blip. But Managements which did not have the right attitude will try to get round the rules rather than conform to the new higher standards.

More control rarely changes poor behaviour!

Risk Management

The Changing Role of Internal Audit

An interview with *Sarah Blackburn*
***(formerly Head of Global Audit and Assurance, Exel plc)* and**
Richard Nelson, President of the Institute of Internal Auditors

Sarah Blackburn was until recently Head of Global Audit and Assurance at Exel. After her first taste of internal audit with Sainsbury's, Sarah headed up internal audit in Argos plc, Kingfisher plc and then Lex Service plc. She has specialised in re-establishing and re-energising internal audit departments, bringing a risk based approach and client-centred working. She has written three books on internal auditing and risk management.

Richard Nelson is President of the Institute of Internal Auditors, – UK and Ireland (IIA), a body which has over 6,000 members and represents Internal Auditors throughout the UK and Ireland. He has worked for many years in Internal Auditing in a variety of companies from a Regional Electricity Board to a firm of Chartered Accountants to British Gas in its various forms over the years since it was privatised. His last post was as Head of Audit for Lattice plc, one of the companies formed from British Gas and the owner of Transco which runs the UK gas pipeline system. While at British Gas Richard devised the risk management system used by BG and its successor companies and the risk based Internal Audit approach currently in use.

The way in which internal audit has widened out as a discipline into a whole raft of risk management skills has been one of the success stories of the last decade. Sarah Blackburn who, until recently was head of global audit and assurance at Exel, makes the point clearly. 'Internal audit began as a financial policing function', she said, 'and a whole service of control grew up around it'. This narrow focus could not survive. 'That idea was eroded from the start', she said. 'Auditors were thinking more broadly. You came to realise that where the problem you were looking at had started wasn't necessarily in the finance department'.

This was the start of a growth in the understanding of what a useful service internal audit provided and how it would be transformed as more and more reforms of corporate governance made themselves felt. 'Since the Turnbull Report and Combined Code were introduced in the UK', said Blackburn, 'you have had the idea of the importance of independent assurance. It is a question of how can a rigid control framework sit with a flexible and dynamic organisation'.

It has become a central part of the art of risk management. 'There is a need', she said, 'for understanding of what the risks are and the nature of the organisation's response. The organisation now needs to cultivate a self-awareness'.

Richard Nelson, president of the Institute of Internal Auditors, agreed. 'There has to be a much greater focus now on how the internal auditor can help the board of directors and the company's audit committee', he said. The reforms have turned the old process on its head. Traditionally the board of directors saw internal audit, if they saw it at all, as a dull but worthy process. It was good housekeeping but it rarely impinged on their decision-making. All that has changed as the reforms have made the outside world much more aware of the

risks which companies face. Boards of directors have realised that there are consequences to the principle that the buck stops with them.

'What is changing', said Nelson, 'is the nature of the assurance that the board needs. This applies especially to the non-executive directors who are spending a relatively small part of their time with the company'. The non-executive directors are worried by the way that blame is being handed out in the corporate world. 'So there is a much greater appreciation by non-executive directors', said Nelson, 'that they should be using the internal auditors for their assurance'.

Blackburn agreed. Internal audit was the automatic destination if people were worried about assurance. 'Internal audit provides independent assurance to non-executive directors that the management is doing what it is telling you it is doing', she said. 'That is a really strong role for internal audit'.

Changing internal audit processes

This extension of the need for assurance by all stakeholders is likely to widen the role even further. 'Should internal audit be commenting on the work of the external auditors ?', asked Nelson. 'I think that there is a role for the effectiveness of the external auditors to be reviewed and the heads of internal audit in companies should have a view because they will have a close relationship with the external auditors'. There are also other issues in a post-Enron world. 'The audit committee should be ensuring that they have a good understanding of the other consulting work the external auditors are doing', said Nelson. 'Internal audit should be asking the questions'.

Blackburn's view is that we are not seeing just a swing of the pendulum but a real sea change. 'Independent assurance is here to stay', she said. 'The non-executive directors and the audit committees now have to say: "Are you really looking at this ?". The non-executive directors are looking for more assurance from whatever source they can get and internal audit is at the heart of that'.

This is leading to changes in the internal audit process. 'There is a much greater shift towards internal audit using a risk-based approach', said Nelson. 'In the past the internal audit department would say "well we will select a system and review when we last looked at it". Now they are focusing on what the company sees as its major risks'.

In its turn this is leading to different strands of responsibility. 'Internal audit should be reviewing the risk management processes used through the company', said Nelson, 'and it should be used by management to identify the risks and the probabilities. But controls of those risks should be put in place by management and internal audit should be questioning those controls. Internal audit should be able to stand back and say: "Are these the right controls"'.

This is a complete turnaround from the days when internal audit was a subservient and bureaucratic process. 'It is much more helpful and beneficial to management than the old internal audit approach', said Nelson. And that should also provoke a change in attitude at boardroom level. 'Management now sees internal audit as being there to help', he said.

Internal audit reporting

There also needs to be a reassessment on the part of internal audit. 'Internal audit now needs to think about how to report to audit committees and boards of directors', said Nelson, 'using the Turnbull report as a template'. And not only does the whole reporting approach have to be changed or modified – the changing

needs will force different criteria to be used. 'Internal audit should produce probability ratings for the audit committee', said Nelson, 'and then prioritise and give the audit committee a greater say on how much resource is needed to look at whichever level of risk is appropriate'. Blackburn can also see internal audit expanding back to its old heartland. Again the question is of resources and where they can best be applied. 'People are saying that internal audit should go back in part to substantive testing and detailed work', she said. 'But there have to be the resources to do these things'.

For audit committees to understand these pressures better communication must be applied. 'Greater dialogue with the audit committee about the level of assurance that they require will be needed', said Nelson, 'and there will be pressure on the head of audit to say how effective the risk management controls are'. It has become a much more demanding and pressured world. 'Audit committees', said Blackburn, 'have become much more demanding. They are keeping chief executive officers and internal auditors on their toes. It is all part of the equilibrium needed'.

This in turn could lead to a change in emphasis. 'It could lead to an audit committee which specialises in internal auditing affairs', said Blackburn. But resources and who provides them is at the heart of this reform. 'At the moment audit committees only get the resources that line management says they can have', she said.

And there are other issues appearing all the time. The extension of the provisions of the American Sarbanes-Oxley legislation on corporate responsibility to leading companies around the globe has, for example, made people more nervous. In particular, they worry about criminal sanctions being attached to directors signing off the figures. 'Chief executive officers and chief financial officers are being asked to sign in blood', said Nelson. 'There will be a much greater call for auditors to do work in these areas and review the financial statements further. In many companies these things are only looked at by the external auditors. Now there will be an internal process as well. It gives the board', he said, 'pause for thought'.

All this has expanded the role of internal audit. 'From the internal audit perspective', said Nelson, 'internal auditors are seen as the experts on internal controls. Now they are being looked upon as the experts in risk management as well'. And that means a greater challenge. 'Internal audit', he said, 'needs to meet these additional demands'.

Expanding responsibilities for internal audit

Blackburn would point to an even greater extension of the role and responsibilities of the internal auditor. 'The broadening of the approach expands the role of different experts', she said. 'Internal auditors are already expert in financial controls. Now they need to become experts in the softer controls'. By this she means the way that an internal control and risk management culture can provide assistance in areas undreamed of by the traditional internal audit department.

'We should be looking at ways of changing the company for the better', she said. 'It is management's responsibility to do this but internal audit could help. It could provide the role of coach. It could provide feedback and encouragement and help management to reflect on events. 'It is', she admitted, 'an ocean away from the training you get as a young accountant. But it can work'.

She also saw a world where risk managers could provide assurance beyond the narrow remit of the company. 'The assurance we provide at the moment is internal', she said, 'and the external auditors only owe responsibility to the shareholders. But society demands accountability. Who reports on that ? As a citizen I want to know more. I want to know, for example, that the company cares about the sustainability of the economy'.

It is a world away from the old view of the internal audit department. But it is the direction in which corporate responsibility and the inexhaustible demand for assurance is heading.

Risk Management

Dealing with Information Risk

Robin Mathieson CA, MBCS

Robin Mathieson was formerly IT Director of the Institute of Chartered Accountants in Scotland and is now an independent consultant, acting as Technical Manager to the IFAC FMAC and SMP Task Force

Information has arguably become one of the most important assets a business can possess. It is now commonplace – if not clichéd – to say we live in an information age.

Information can exist in many forms – spoken word, as items printed or written down or contained in videos. This article is primarily concerned with information stored and transmitted electronically. Indeed, for a number of firms, data stored in their computers or on public and private networks is their chief and most valuable asset.

The need to control the flow of business information in organisations is not new. The possibility of fraud and error has always existed and such risks needed to be controlled or mitigated.

Risk appetite/risk literacy

However, as companies across the world become more and more dependent on IT, this risk has become compounded. Mission critical systems processing information over rapidly expanding networks can affect the integrity, availability and confidentiality of information resources. Electronic commerce and more recently mobile commerce across wireless networks have created additional layers of complexity.

However, information security is not simply about encrypting data or creating firewalls, even though these can be crucial in any attempt to ensure greater security. It needs to be viewed in the context of the organisation-wide risk management strategy.

The issue is not an individual hacker or a deadly virus but a company's overall policy. Technology on its own can produce tactical solutions but does not by itself engender good business practice. Indeed, many of the problems attributed to IT are in fact management issues and should, therefore, be the responsibility of the organisation as a whole rather than the IT department.

In fact, the Turnbull report in the UK stipulated that limited companies must be able to demonstrate a rigorous system of internal control for information assurance. In that sense, information security should be an item on the corporate governance agenda. Such top down approach may seem misplaced for an issue that may be too 'technical' for most board directors. Yet in a world where IT can be a real source of competitive advantage, it is the only way to ensure that information security risks are aligned with overall corporate goals.

The Canadian Institute of Chartered Accountants (CICA) recently produced a document entitled 'Twenty Questions Directors Should Ask About IT'. The introduction states:

The board of directors oversees an organisation's overall strategic direction and management. As part of this responsibility, it must keep abreast of issues pertaining to the management and control systems in place to keep the risk of loss arising from fraud and error to an acceptable level. Board members must monitor those systems and ask the right questions to ensure that systems are operating as they should.

Among the areas highlighted, the CICA guide singles out the following:

1. Strategic planning for the information systems (IS) area.
2. Tracking technological trends to regularly update hardware and software.
3. Performance management systems for IT.
4. Programmes for hiring and retention of skilled personnel.
5. IT corporate governance.
6. Risk and security.
7. Personal information privacy, including legislative requirements.
8. Risks and controls of e-business activities.
9. Availability, including business continuity and formal recovery plans.
10. Legal issues such as software licences.

Clearly, this list covers a broad spectrum of IT-related issues that need to be managed but points 6–10 focus specifically on risk and security covered by this article.

The Department of Trade and Industry of the UK Government sums up the problem of IT security rather neatly:

Increasingly, organisations and their information systems (both manual and computerised) are faced with security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, fire, flood and other disasters. Computer viruses and computer hackers are a continuing threat. The majority of serious security incidents are commonly described as 'accidental' – a term which can include carelessness and ignorance.

Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage, maximise returns on investment and business opportunities.

There is no shortage of materials available on individual aspects of information security. For example, ISO 13335 – produced by the International Organisation for Standardisation – is a five-part technical report (not a Standard though) entitled *Guidelines for the Management of IT Security* – commonly referred to as GMITS. It covers the following areas:

1. Concepts and models for IT security.
2. Managing and planning IT security.
3. Techniques for the management of IT security.
4. Selection of safeguards.
5. Management guidelines on network security.

The other key text in this area is a *Code of Practice for Information Security Management* BS 7799. Part 1 of this Standard outlines best practice in security controls in implementation and enhancement of information security for businesses and government. Although fairly old, it was updated and revised in 1999 to include new technological developments, principally e-commerce. Due to international interest, BS7799-1:1999 was published in December 2000 as International Standard BS ISO/IEC 17799. It has been adopted for domestic use

in Australia, New Zealand, The Netherlands, Czech Republic, Denmark, Korea and Sweden and is available in French, German and Japanese.

Part 2 of BS7799 is currently being revised. It was first published in 1998 (BS7799-2:1998) and defined a process for developing and establishing an information security management system specifying controls to be implemented according to security, legal and business requirements. In addition, it could be used to conduct internal audits and third party specifications.

The Standard as a whole defines information security as the preservation of confidentiality, integrity and availability. This is achieved by implementing a suitable set of controls, such as policies, practices, procedures, organisational structures or software functions.

Security requirements can be identified by a methodical assessment of security risks. Of course, the cost of control procedures needs to be balanced against the business harm likely to result from potential security failures. In addition, risk assessment techniques may be applied to the whole of the organisation, parts of it, individual information systems or specific system components or services, where practicable and applicable.

Once security requirements have been identified and prioritised, controls need to be reviewed or selected and implemented to ensure risks are reduced to an acceptable level. There are many ways in which this could be done and BS7799-1 in particular provides some good examples. Whichever way is chosen will depend on the company's previously established risk appetite and the chosen method of reducing risk.

It is not the purpose of this paper to go into details of how information security management systems can be developed or improved. In any case, there is no one universally applicable solution that would fit every organisation – which is why initial risk assessment is crucial. Instead, it aims to raise awareness of information risks.

Management must be committed to developing, implementing and improving the effectiveness of organisations' systems so that business, legal and regulatory requirements are met.

Instead of technological solutions alone, then, what is needed is good business practice. To make the process more effective, staff throughout the organisation should be made aware of and responsible for information security. No system will ever be completely foolproof but putting IT on the corporate governance agenda will go some way in ensuring information security risks are mitigated, controlled or indeed exploited.

Risk Management

Is Better Risk Disclosure the Next Step for your Company?

Stathis Gould MBA, Head of Technical Issues, CIMA

Stathis is responsible for representing members' views in response to government and other consultations relevant to the profession and for the technical programme of guides and briefings. He has worked in both the private and public sectors, including a US translation and software localisation company providing multilingual services, the NHS, and the British Dental Association.

Consider the following two statements and your views on them:

(a) Robust risk management adds value to your organisation because it helps maximise shareholder value at the same time as reducing the probability of financial failure.

(b) Your company can gain from disclosing to shareholders the significant risks the firm faces and actions being taken to manage these. The main benefits are a reduced cost of capital for a company and increased management capability.

I would be surprised whether many executives and managers would disagree with the first statement. Many would probably contend the second statement. Risk disclosure is an awkward debate for company leaders but one which will have to be faced increasingly in the future. The focus over the last few years has been on ensuring an effective internal risk management framework. Now the focus is turning to how much you can tell investors about the outcomes of the risk management process.

The principal agent problem discussed extensively by management and economics theorists stems from information asymmetry between company management and shareholders. The information asymmetry between some executive and non-executive board members and the resulting powerlessness of non-executive directors in fulfilling their monitoring role effectively demonstrates the problems of unfettered decision-making. In the same way, some investors argue that the lack of transparency inhibits their ability to take action and to proactively manage their investment portfolios. Many fund managers have been asking for more predictive and faster information and the implementation of earlier warning systems to help them reveal early signs of decline or growth opportunities.

Current level of risk disclosure

Better risk disclosure and more business transparency is a dilemma for many companies. This view manifests itself in the many bland, high level descriptions of their risk management processes that companies provide in their annual reports and operating and financial reviews.

In the UK, the Turnbull report in 1999 aimed to provide a conceptual framework for companies to identify, evaluate and manage significant risk and that procedures for doing so are reviewed regularly. While Turnbull's

guidance may have led to many companies improving or introducing internal control and risk management processes, its failure to require companies to disclose or discuss the actual risks they are facing has led most UK companies to do one of two things:

1. Provide mundane statements or 'boiler plates' describing internal control procedures which never change much from one year to the next. Such statements are not particularly meaningful or relevant over time; ***or***
2. Provide dynamic narrative statements that demonstrate that there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company and that this is regularly reviewed by the board. The intention is to demonstrate that a company has a system of internal control which is designed to identify and lead to management action over the risks that threaten the achievement of business objectives.

As Table 1 indicates, only a few UK companies have chosen to disclose significant business risks facing their companies.

Table 1: Developments with internal controls in the UK

Of 342 companies analysed, 84 per cent address their internal controls and the table sets out the most popular areas being disclosed

Internal controls disclosed	*%*	*Selected companies*
Substantive business risk disclosure	14	BHP Billiton, Barratt Developments, George Wimpey, Hays, MWB, NXT, Victrex
Limited business risk disclosure	63	Diageo, Hanson, Scottish Power, Smiths, Standard Chartered, WH Smith, Wolseley
Disclosure of business environment	11	API, Allied Domecq, BHP Billiton, Enodis, Logica, MWB, Sage, Scottish Power, Synstar, W H Smith
Information and communication systems	15	API, BHP Billiton, Crest Nicholson, Hanson, Hoildaybreak, Northern Rock, Standard Chartered
Control procedures	62	Allied Domecq, BHP Billiton, Diageo, Hanson, Hayes, Scottish Power, Smiths, W H Smith, Wolseley
Monitoring process	44	Allied Domecq, British Sky Broadcasting, Carlton Communications, Chubb, Scottish Power
Financial reporting	26	BHP Billiton, Carlton Communications, Chubb, George Wimpey, Hanson, Trinity Mirror

Note: (i) the percentage figures are based on the number of companies with internal control disclosures and (ii) companies disclose in more than one area

Source: *Company Reporting,* No 145, July 2002, p. 4

Commentary for Table 1

What risk disclosures might be necessary?

Business risks generally fall into five groups: strategic, financial, operational, commercial and technical, although there are a number of ways of categorising risks. More importantly, risk factors tend to be hard or soft where soft factors such as poor choice of market are not easily subject to quantifiable analysis. It is often these soft factors and non-financial risks that lead to poor corporate performance or failure. These are the sorts of risks on which investors are often kept in the dark. Furthermore, relatively few companies undertake any extensive discussion of the business environment that they face and the challenges that lie ahead. This is arguably one of the most important areas that fund managers would like information and views on from companies.

Whatever your view on risk reporting, investors cannot make a very informed judgement from bland disclosures as to whether a company has a sound system of internal control. Even if there is a statement to the effect, 'We have an effective internal control procedure', included in the annual report. Such statements although benign are meaningless, giving no indication whether an effective continuous risk management process is in place. Nor do detailed descriptive statements demonstrate whether a company is actually aware of, and understands, the material risks facing the business. These too can be argued to be of very limited relevance to investors. But at least they can convey an acknowledgement of the importance of risk management in terms of the success in the organisation.

The Institute of Chartered Accountants in England and Wales has argued for a number of years that companies should use the results of their risk management process to ensure that they are giving investors a complete picture of the company's business risks and how they are being managed.

There is no doubt that this should be possible because a company with a robust system of internal control will have:

- understood the nature of the risks facing it;
- decided the extent and categories of risk which it regards as acceptable for it to bear;
- considered the likelihood of the risks materialising;
- judged its ability to reduce the incidence and impact on the business of risks that do materialise; *and*
- estimated the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.

The reality is that a majority of companies that choose to disclose their board approved policies to manage risks, tend to focus narrowly on the following types of risk:

- interest rates;
- credit;
- foreign currency;
- funding and liquidity;
- commodity prices.

This brings them into accordance with the UK Financial Reporting Standard 13 or IAS 32 Financial Instruments: Disclosure and Presentation, or FAS 107 Disclosures about Fair Value of Financial Instruments and FAS 133 Accounting for Derivative Instruments and Hedging Activities, which requires company disclosures to provide information about the impact of financial instruments on the entity's risk profile, how the risks arising from such

instruments might affect the entity's performance and financial condition, and how these risks are being managed.

The objective of financial risk disclosure is to demonstrate how a company has reduced the potential loss related to such risks and the financial instruments such as derivatives deployed to hedge these. Such disclosure is important because targeted financial instruments and insurance can reduce or eliminate the effect of such risks on firm value. Certainly for banks, a detailed analysis of credit risk profile by industry, region, division, and defining a key measure of market risk such as 'value at risk' (VaR), and providing analysis of trading income against VaR over time is useful. However, disclosure would be more effective, if there was disclosure on how long-term performance could be affected by a wider set of strategic and operational risks facing the company, which could prevent implementation of its strategy and discussed in the context of the market environment.

It is also interesting to note that in the UK, prospectuses produced by companies seeking flotation generally offer detailed risk disclosures so investors are aware of all material information. There is reluctance by directors to produce such a level of disclosure in annual reports. Risk disclosures concern many company directors for the following reasons:

- price and commercial sensitivity of information;
- business risk too complex to capture in a report;
- annual reports already too long – danger of information overload;
- many users of company disclosures not sophisticated enough;
- forward looking information could be misconstrued as a definitive forecast and potentially investors make future investment decisions based on it;
- if risks are significant, disclosure should be made before the annual Operating and Financial Review (OFR, Management Discussion and Analysis in the US) because the main focus of analysts and institutional investors in relation to the annual results is the preliminary announcement;
- better disclosure may not reduce a company's cost of capital.

Of all the potential obstacles to improved disclosure, three are particularly hard to address. First, there is no doubt that most directors feel that by providing comprehensive risk disclosures, they could be held hostage to fortune if future events are unanticipated. Second, there is a deep-rooted fear that in disclosing risk information, whether strategic or operational, competitors will be provided with intellectual property that they may use to enhance their position. And third, companies do not often have a clear vision of what investors would like to know. If they do, in the first instance, it can be an onerous task getting the necessary management information into the boardroom.

The status of reporting in the USA

The USA's litigious society has led to a trend of seeking verification by lawyers for any disclosure statements. The advice generally given to UK companies with US listings is to take the minimalist approach to risk disclosure in respect to 20-F annual report filings. The operating and financial review (OFR) of companies having US listings tend to be constrained and less forward looking because US legal advisers expect evidence to support every assertion being made. US companies, in their version of the OFR, the Management Discussion and Analysis (MD & A), are even more constrained than their UK counterparts in providing narrative discussion on business performance and assessing the future potential of the business. Again, the boiler plate approach adopted by many American companies in their MD & A stems from the dominance and advice of legal advisers within a litigious society.

Investors' attitudes

In the entire debate on improving disclosure of risk in company reporting, there has been little analysis on whether users of financial reports have strong preferences for the disclosure of particular types of risk. In empirical research undertaken by Cardiff University involving 552 institutional investors, almost a third displayed a strong need for increased corporate risk disclosure that would help to improve portfolio investment decisions. For others, their information needs were probably being largely satisfied by private disclosure through one-to-one meetings with company management although their attitudes tended to be associated with the specific characteristics of the funds managed and the investment horizons. Those institutional investors that require greater disclosure also viewed corporate governance as a way of improving corporate performance rather than simply as a system of control. It is also the view of some that narrative disclosures such as those contained in the OFR attract wide readership from private shareholders.

McKinsey & Company's 2002 Global Investor Opinion Survey on Corporate Governance showed that an overwhelming majority of institutional investors are prepared to pay a significant premium for companies exhibiting high governance standards. If this was to be the case with risk management, companies would have to do a better job in demonstrating the effectiveness of their risk management and this would probably involve appropriate detail to substantiate their judgement that their internal controls are effective.

Motivation for better disclosure

The introduction of a revised and mandatory OFR in the UK could be set to change directors' views on reporting and risk disclosure. The OFR, as proposed by the UK Company Law Review, and now being developed by the Accounting Standards Board, will require companies to improve their reporting in the following areas:

- The company's business and objectives, strategy and principal drivers of performance.
- A fair review of the development of the company's and/or group's business over the year and position at the end of it, including post-year-end events, operating performance and material changes.
- Dynamics of the business – i.e. known events, trends, uncertainties and other factors that might substantially affect future performance, including investment programmes.
- Corporate governance – values and structures.
- An account of the company's key relationships, with employees, customers, suppliers and others, on which its success depends.
- Policies and performance on environmental, community, social, ethical and reputational issues, including compliance with relevant laws and regulations.
- Receipts from and returns to shareholders.

Although the OFR will be one reporting framework, it is likely to lead to a number of reporting models for different industry sectors. Standards for information quality could well emerge for different sectors.

Rather than issuing detailed mandatory requirements, the OFR will probably focus on directors' judgement to provide a relevant account of their company's performance. In this respect, the reporting of risk will be covered by the OFR – not specifically in one section – but rather should be captured in the various areas of the OFR. This is a positive step in improving transparency by enhancing public reporting to stakeholders on long-term issues. It will certainly be an opportunity for companies to talk more about the business and operational risks that the business is facing in the context of the strategic direction being adopted by a company. If companies were not allowed freedom to determine to some extent what to include in their OFRs, directors who are concerned

about risk disclosure and are under pressure to conform to rules, will probably produce uninspiring lists of risks that could apply to any company in any sector.

Besides, this is an opportunity to improve stakeholder reporting more generally. The debate on disclosure always gravitates on one major issue – how to strike a balance between too much disclosure and too little. The best way forward will be to allow those companies taking the lead to create market pressure on others to improve. It will increasingly become the case that poor quality dialogue could damage reputation.

It will always be the case that some companies will be increasingly prepared to be more open and transparent and this is demonstrated by PricewaterhouseCooper's *Value Reporting Focus 2002* which reviews companies which are leading external reporting. Those companies experiencing good performance and profitability naturally tend to be more transparent and this should also particularly be the case for companies with already public business models and strategies. The logic is that following a thorough implementation of Turnbull recommendations (if in the UK), all companies should be in a position to demonstrate that their internal risk management and internal control processes are working effectively. This is fundamental to increased risk disclosure if a company chooses to pursue this course. The crucial issue for all stakeholders is that internal procedures actually add value and inform the business. As we are seeing with corporate social responsibility reporting, leading companies will want to distinguish themselves from the rest of the pack. For these companies, the goal will be for a seamless interface between management accounting, external reporting and investor needs.

Some people argue the real difficulty will surround the verification of what is being disclosed. Under current proposals, the process behind compiling the OFR will be audited. External auditors can focus on the process of internal control and risk management so to ensure a robust framework is in place. Is this a sufficient independent test to verify that there has not been misinformation reported? This is an issue that may concern some. However, like many other performance issues, much will always depend on the morality, integrity and good judgement of executives and managers. And, of course, there is the analyst and investment community. They have a part to play in judging for themselves the quality of reporting.

Risk Management

Risk Management in the Public Sector

Carole Hicks, Finance and Policy Manager, CIPFA **and**
Stathis Gould, Head of Technical Issues, CIMA

Carole Hicks is the Finance and Policy Manager at CIPFA covering financial management issues. Previously, she worked as a Research Fellow at the Centre for the Study of Regulated Industries on regulatory and accounting issues in the privatised utility companies and as an accountant in a number of UK Local Authorities.

In the last few years, the UK public sector has witnessed a surge of interest into the practices of risk management. Government departments and agencies are now expected to have risk management systems in place and produce a 'Statement of Internal Control' modelled on the Turnbull guidance for private sector companies. Similar assurance into the adequacy of risk management is also required in the NHS, local government, education and social housing sectors.

The catalyst for this interest has been a reaction to the private sector's response to governance failures such as BCCI, together with the Labour Government's new agenda and its wide reaching programme of reform. The White Paper entitled *Modernising Government* was published in 1999 and set out the government's vision for public services into the 21st century. It explicitly encouraged new ways of doing things in the public sector, with a view of creating a more entrepreneurial, risk-literate culture.

The introduction of Best Value in the UK, the creation of quasi-market organisations such as Executive Agencies and new partnerships with industry in projects such as Private Finance Initiative (PFI) are just some of the developments which have generated additional risks in the public sector. Public Service Agreements and the setting of performance targets have put even more emphasis on issues of accountability. Resource accounting and budgeting is now in place and means that government departments are now being charged for their use of capital assets. In tandem with the more business-oriented accounting and performance measurement systems has come the thrust for continuous improvement. Identifying risks, making explicit the ownership of those risks and assessing their likely impacts is a key feature in the new landscape.

At the same time as these changes have been happening in the public sector, the way in which risk is viewed in the private sector has been changing from risk minimisation to risk optimisation. Risk management has thus become not only the first line of defence against corporate failure but also an opportunity to generate shareholder wealth. The main message of the Turnbull report was that reduction of surprises and increased ability to meet objectives should lead to a higher share price and a lower cost of capital. Importantly, both 'good' and 'bad' risks are mentioned – the greatest hazard being not taking any risks at all.

In addition, we have seen an increase in risks that affect public and private sectors alike. The risks associated with IT, for example, can translate into both the operational ones of when to purchase the most up-to-date hardware and software as well as the strategic risks of failing to provide additional channels of delivery. Similarly, the ascent of the so-called blame culture has meant that people expect compensation if anything goes

wrong – negligence claims in the National Health Service (NHS) continue to rise and are a drain on the additional resources earmarked for improvement.

The Modernising Government agenda, together with a wider change in the business environment, have naturally led diverse public sector organisations to focus on risk management. In reality, there has always been some sort of risk management in the public sector but many of the risks were not made explicit or fed into the planning process.

The benefits of managing risk may initially be less clear than in the case of profit-driven companies. However, all public sector organisations have objectives and targets which must be reached if they are to retain the confidence of their funders. They too need to add value to their services. The criteria of success may be different – access, availability and equity in service provision rather than financial performance – but they are engaged in what is essentially the same process. They need to meet their outputs and protect their assets, including intangible ones, such as reputation.

For example, the commonly used phraseology in the NHS talks about organisations having risk management and control assurance processes and systems in place, to enable them to give assurances that they are doing their reasonable best to manage themselves, so as to meet their objectives and protect patients, staff, the public and other stakeholders against risks of all kinds. There is also a frequent reference to providing assurance that affairs are managed efficiently and effectively.

CIPFA in its 2001 publication *Risk Management in the Public Services* examined how organisations might make risk management an integral part of their management processes, in much the same way as human resources management is integrated at all levels within organisations.

The nature of the public sector means that perceptions of risk can be very different. It is often the case that public reaction to a threat is unrelated to its actual level of seriousness or its consequences. For example, although the risks of travelling by car are still far greater than those of using trains, the public's reaction to the recent train disasters has been to demand an almost 100 per cent safety record. It is clearly difficult to balance the necessary caution (coupled with accountability for public money) with creating a less risk-averse culture.

There are various prescribed ways of establishing a risk management framework but it is important to remember that many risks are organisation or market-specific. This is why neither Turnbull, nor any of the other risk management guides, offer an off-the-peg strategy.

On the other hand, because a service focus in the public sector will frequently not map neatly onto the boundaries of an organisation, it is worth considering cross-organisational or departmental risks too.

CIMA's *Risk Management – A Guide to Good Practice*, published in October 2002, recommends taking a number of iterative steps in a risk management cycle:

1. Establish risk management agenda group and set goals.
2. Identify risk areas.
3. Understand and assess the scale of risk.
4. Develop a risk response strategy.
5. Implement the strategy and allocate responsibilities.
6. Implement and monitor implementation of the suggested controls.
7. Do it again!

The overarching framework should be that any risk management system is tied in with the overall strategy and objectives, embedded throughout the organisation and refined on a regular basis.

For this process to be successful, there also needs to be a change in the overall culture of the public sector. In a recent United Kingdom National Audit Office (UK NAO) report, 41 per cent of the government departments surveyed still claimed they considered themselves to be risk-averse.

The same report showed that in just over 40 per cent of departments, all staff have responsibility for identifying and managing risks. That leaves over half where risk management is presumably seen as a senior management objective. It is worth remembering that risk management – and corporate governance as a whole – is of little value if it simply turns into another compliance issue or a bolt-on to everyday operations. It should not be driven by regulation or fear of audit scrutiny. Instead, it is about creating a culture open to innovation. As such, it should form an integral part of strategic planning as well as first-line operational management.

For that very reason, risk management frameworks should not be overly complicated, even though risks themselves are rarely straightforward. Concentrating too much on developing complex models risks alienating the majority of employees.

In fact, companies in the private sector are increasingly abandoning complicated numerical systems in favour of simple and more understandable approaches that rely on the 'collective wisdom' of the company as a whole. This does not mean that all measurement should be abandoned altogether. It is simply that the public sector should not fall into the trap of making risk management the proverbial rocket science .

Managers in the UK NHS, for example, have established some of the most advanced measuring mechanisms in the light of increasing clinical negligence claims. Nevertheless, there is an admission that there is still a long way to go in creating the kind of culture that would make these tools function effectively.

Clearly, there is a lot to be achieved but the foundations of successful risk management seem to be in place throughout the public sector. The UK NAO report shows that most government departments are familiar with the theory behind it, although they seem less clear about its tangible benefits or how to apply it in practice.

The priority for the government should be to translate this awareness into a sound practical knowledge. Less than 20 per cent of those surveyed by the UK NAO claimed their organisations had effective training programmes in place. If this is not rectified, formal guidelines are unlikely to be implemented. Principles of risk management should be incorporated into existing training programmes at all levels, from induction to tailor-made courses. Risk management can thus become a part of the everyday business language of an organisation.

Government insistence on risk-taking may appear to be pulling the public sector in two opposing directions. On the one hand, it is being urged to be more daring and on the other, it is subject to increasing public scrutiny.

A good example of this is the Millennium Commission, a government body set up in 1993 in charge of investing lottery funding into various projects. Spending public money means that it has to be risk-averse but its mission is to fund forward-looking projects and that in turn means backing innovative ideas. The lottery is played throughout the UK so money has to be spread across the regions, which increases the risk of failure. Its director and accounting officer Mike O'Connor says: 'We have to balance prudent risk taking with the need to innovate. (…). You model all these things as best you can. But it doesn't matter how much work you do, you won't come to an answer that is risk free.' (*Accountancy Age*, 2000)

In other words, prudence and innovation are not mutually exclusive. Finding the right balance between them is precisely what sound risk management is about.

Risk Management

Implementation of Risk Management in the Public Sector

A case study of the Australian Victorian Department of Natural Resources and the Environment , CPA Australia

Risk management is now an integral component of effective organisational management. Acknowledging its broad accountability and the potential crises that could stem from not addressing this issue, the public sector in Australia has been actively pursuing risk management strategies since the mid-1990s, with many agencies taking a proactive lead.

The following synopsis is one of the case studies from CPA Australia's publication, *Case Studies in Public Sector Risk Management,* which looks at the Victorian Department of Natural Resources and Environment's (DNRE's) key risk management processes. The extract examines DNRE's drivers, implementation, successes, lessons learned, future directions and implications within a public sector arena.

The Victorian Department of Natural Resources and the Environment

The Department of Natural Resources and the Environment (DNRE) encompasses the portfolios of Environment and Conservation, Agriculture, Aboriginal Affairs and Energy and Resources. It is responsible for the development, conservation and protection of the state of Victoria's natural resources.

With over 4,000 staff in Victoria in more than 200 locations across six regions, the Department incorporates diverse functions that have the potential for conflicting priorities. It also regulates increasingly sophisticated industries that impact the community on a daily basis.

The 2001–2002 objectives for the Department (Budget Estimates 2001–2002) include:

- the management and protection of Victoria's natural resources;
- developing and facilitating policy development and discussion in relevant areas (such as greenhouse gas emissions and mad cow disease);
- provision of policies to facilitate sustainable and competitive resource use;
- demonstrable leadership and stewardship in the portfolio areas;
- a whole-of-government approach to improve Aboriginal wellbeing through partnerships to achieve Aboriginal aspirations for land, culture, heritage, family and community;
- increasing the Victorian community's access to information and engagement in natural resource and environmental decision-making.

The process

The Department was established in April 1996 by bringing together ten former organisations. The new entity effectively became ten major businesses within one organisation that reports to three ministers. To add to this complexity, the Secretary of the Department also has responsibility for a number of statutory bodies who

generally report to particular ministers and which are outside the department itself but within the broader portfolio framework.

A recognition by the DNRE executive of the potential risk management exposures and opportunities, accompanied by an increasing awareness of legal exposure and insurance issues, led to the Department developing a risk management strategic framework to support its corporate governance and strategic business planning processes.

The Department has structured the implementation of its risk management framework around the following stages:

1. formulation/policy development (February 1997 to July 1999);
2. implementation (March 1999 to March 2001);
3. sustainability and convergence (February 2001 onwards).

1. Formulation

The Department's framework is based on the AS/NZS 4360:1999 Risk Management Standard. Developed in-house, utilising the skills of a policy development expert, the key features of this framework are:

- identification of objectives – for a project, activity, program, business unit or the Department as a whole;
- pinpointing the risks associated with achieving these objectives;
- implementing ways of dealing with these risks to ensure that the objectives are met in an appropriate manner.

This stage of the project was managed by a risk management committee, formed from the audit committee of the Department.

The framework emphasised the identification and management of risks on a day-to-day basis, as well as the development of a culture that optimises the Department's ability to achieve business objectives while managing risk.

2. Implementation

The implementation phase of DNRE's rollout has been based on self-assessment and continual reassessment.

The Department was split into 23 segments, reflective of policy and operational responsibilities. Risk management coordinators were appointed and trained to oversee the implementation process in each segment. These coordinators have an ongoing role of coaching and facilitating the development of risk management and risk treatment plans.

All levels of the Department were targeted, with over 700 staff involved in the programme to date. Workshops were conducted across the 23 segments to discuss risk identification and assessment, and also receptivity to risk, and its treatment.

Initial workshops were held with the Department Executive and targeted corporate risks (those that impacted more than one segment of the Department). Workshops were then held with divisions and regions. These examined both corporate and division/region specific (local) risks.

Initially, the workshops resulted in the identification and highlighting of over 500 risks for both the Department as a whole and its components. These have been reviewed and aggregated down to 100 at the present time, with more reviews and analyses planned for the near future.

Treatment plans have been developed and all the information collected from the workshops has been contained in an electronic format to permit automatic input to a risk management database. This database contains:

- risk treatment plans – local, project and corporate;
- a risk register;
- risk profiles.

The database also has the capacity to assist in the development of treatment plans through providing step-by-step templates for completion of plans in this process.

While the database has potential, the current software application is not sophisticated enough to meet all needs. The Department has acknowledged this and is examining alternatives.

It was noted that the staff in the Department tended to be fairly self-critical during the self-assessment process, which includes making informed judgements about the control environment. Overall, however, the risk profile for the Department matched that of similar organisations.

3. Sustainability and convergence

The Department is now seeking to completely embed risk management into its operations and culture in order to practise good business and support service delivery in an ethical, accountable and transparent manner – captured as a key corporate objective.

This phase will see risk management fully incorporated within business and strategic planning through:

- embedding risk treatment plans into the planning cycle;
- ensuring that risk management is considered in the development of business cases and other resource planning;
- applying a continuous review philosophy to the risk management strategic framework;
- establishing a self-sustaining capability at both the corporate and division/regional levels to support ongoing review and management processes.

The current planning, development and review cycle is being reformulated to embed the risk management effort. The target is the full integration in the 2002–2003 planning cycle.

The proposed process will see risk being identified, treatment plans developed, resources allocated and treatment plans being built into business plans for 2002–2003.

Currently, risk management is generally not fully integrated with the corporate planning process. The Department recognises the importance of training and communication in this next phase and has recently appointed a champion to further this stage. This Risk Management Coordinator – Corporate, resides within the corporate planning team and will also have responsibility for coordinating the activities of the risk management coordinators within divisions and regions. This role is seen to be crucial in refocusing momentum throughout this final, ongoing phase.

The Department is also initiating a process to measure the impact of risk management on the meeting of client expectations. Internal clients will be surveyed to measure this impact, with auditable measures of success still under consideration. Similarly, DNRE has expectations and requirements that contractors and consultants provide services that are compatible with DNRE's risk management philosophy and practice.

Successes

Overall, the Department feels that the implementation process has been relatively smooth. No insurmountable issues of culture eventuated, as staff were able to see the benefits within their own jobs. In fact, there was a realisation that everybody practises risk management and this is now performed in a disciplined, standardised and better-practice manner.

Given the size and complexity of the Department, the implementation process has run well and should provide a strong foundation for continuing to embed risk management into day-to-day operations. The Department has the advantage of having a highly skilled workforce that has been using risk management over a long period.

Specific examples of the benefits and successful use of the framework follow. These can be categorised according to:

1. Project risk.
2. Division/sub-business unit level risk.

1. Project risk

Within the Agricultural Division, a risk management plan was developed to assist in a particular project involving the seizing of stock that was not being cared for appropriately by the owner. The project team was managing a contentious issue that involved dealing with an individual (the owner) who had a history of mental illness. The project incorporated the coordination of resources from government agencies such as Human Services, police and the local council, with the risk management plan being developed and facilitated by a DNRE risk management officer. Potential consequences identified during the risk planning process included:

- injuries to the staff or owner;
- damage or death to stock;
- an incomplete result (missing stock, equipment failure etc.);
- negative media exposure.

The risk management strategic framework was used to identify and measure risks according to likelihood and impact and develop treatment plans. The project was described as a complete success, with the risk treatment plans being considered vital to the management of a complex assignment.

2. Division/sub-business unit level risk

The implementation of the framework within the Chemical Standards Branch of the Agricultural Division was an open process that involved bringing together all staff for the review.

All components of the framework were utilised, with risk management now being seen as part of the day-to-day working environment of the team. Risk management is today embedded within team business plans and performance plans and staff understand their role in the overall process.

This team has also undertaken a stakeholder review process to validate the risk profile developed internally. Chemical resellers were targeted and were asked to nominate what the key risks were in relation to agricultural chemicals. These risks were then compared to those developed internally, to measure the alignment between the industry segment and government. There was a strong correlation between those developed internally and those identified by the resellers. This promoted the feeling amongst staff that the internal process was valid and relevant to their work.

Lessons learned

Generally, the implementation of the risk management framework within the Department went well. However, some individual comments regarding the process included the views that:

- implementation has stalled; and .
- the formal documentation process was too resource intensive in some instances on a day-to-day basis although it was ideal for use in specific projects to manage risk and ensure that controls were in place.

These appear to be merely communication issues and should be minimised now that a corporate Risk Management Coordinator has been appointed and can market the advantages of the 'sustainability' stage to the organisation as a whole.

With the benefit of hindsight, staff involved recommend the following changes:

- increased allocation of resources up-front to enhance facilitation and management of the process through the various levels of the organisation;
- reduced use of contractors and consultants during the implementation to encourage the development of skills in-house;
- ensuring that the IT environment was appropriate and could support the needs of the project – there are concerns about the ability of the current risk management database to meet the needs;
- managing timing to maintain momentum throughout all stages of the project;
- developing a shortened time-frame for formulation and implementation;
- ensuring that the executive actively support the program and convey its importance to all staff;
- celebrating the successes of the program with the relevant team members and across the Department.

Future directions

The sustainability phase will see risk management embedded within the Department's planning processes. With the support of the executive and the corporate Risk Management Coordinator, any momentum that has been recently lost will be recaptured and the ensuing benefits should accrue.

Implications for other areas of management

Overall, the critical success factors for the risk management project were defined as:

- Commitment and involvement.
- Executive and senior management leadership.
- Training and communication initiatives.
- Sustainability and continuous improvement through convergence with business and strategic planning.

These factors can be seen to permeate the Department and its planning processes, with the result that risk management is no longer seen as a stand-alone process but has become instinctive and forms a part of core day-to-day operations, professional practice and associated standards of care.

Executive management must be seen to be proactively committed to ongoing risk management. The use of risk management through the planning and resource allocation processes should ensure its continuing relevance, impact and assurance provision in achieving corporate objectives.

Achieving Measurement Performance Improvement in a Changing World: The Search for New Insight, KPMG Assurance and Advisory Services Centre, New York 2002.

Solomon, J F; Solomon, A; Norton, S D and Joseph, N L (2000), *British Accounting Review*, 32, pp. 447-478.

'Why too many mergers miss the mark', The *Economist*, 4 January 1997, p. 57.

Further reading

British Bankers Association

- *E-risk: Business as Usual?*

  Sections cover:
  - e-risk and the financial services industry;
  - managing e-risk in a complex global banking group;
  - what are the key issues?;
  - analysis of impact;
  - retail credit risk in e-commerce;
  - e-risk strategy, assessment and mitigation; and
  - crisis, what crisis?

CIMA

- *Risk Management: A Guide to Good Practice,* 2002

  This guide is a practical introduction to risk management and provides guidance on establishing a robust risk management framework. It will also enable senior executives to get to grips with Risk Management and keep up with new practices such as ERM. Specifically, it has been written with finance and line managers in mind who desire risk to become an everyday part of their management process.

- *Business Transparency in a Post-Enron World,* 2002

  An executive briefing that explores the city culture and the behaviour that drives business reporting and how this will need to fundamentally change if faith in capital markets is to be restored.

- *Financial Institutions and Corporate Governance: A Dynamic Model of Corporate Governance,* 2002

  This report investigates a detailed model of the private corporate governance role of financial institutions and how it compares to public corporate governance procedures. It is based on case interviews with 40 large UK FM groups during 1997–2000.

- *Fraud Risk Management: A Guide to Good Practice,* 2001

  This guide considers the problem of fraud, its consequences for business, and the practical steps which can be taken to prevent, detect and respond to fraud. It also includes examples of a fraud policy and response plan which can be adapted for use in any organisation.

- *Perceptions of Trade Credit Control in Mainland China and the UK,* 2001

  This report analyses the contrasting perceptions of trade credit control between Britain and Mainland China. A survey of 106 British and mainland-Chinese managers was carried out with the results being divided into four trade credit control components: information, regulation of customer relations, risk management and control activities. The findings show how opposing approaches can be reconciled and how managers who are aware of potential differences can adapt their controls to allow progress.

- *Accounting for Risk in the NHS*, P Fenn, S Diacon, R Hodges and P Watson, 2000

  This report examines the process of accounting for risk in the NHS and its implications for risk management. It draws on research into accounting issues arising from claims made upon NHS Trusts by patients, staff and members of the public.

- *Corporate Governance: History, Practice and Future*

  An exploration of corporate governance as it is used throughout the world, with consideration of how it may develop in the future.

- *Treasury Management: Tools and Techniques for Countering Financial Risks,* 1999

  This comprehensive overview of the tools and techniques involved in treasury management gives a better understanding of the treasury function. Describing the responsibilities the treasury manager will hold within such a department, it covers the wide range of products and techniques now available to counter such financial risks.

- *Assessing Flexibility in Capital Investment:*
  A Guide to Applying Real Option Principles in Investment Appraisal, 1999

  Following a critique of traditional capital investment techniques, and an introduction and analysis of 'real options', the book shows how – using real life examples – successful application of this new approach can give companies real choices throughout the course of an investment project.

CICA (Canadian Institute of Chartered Accountants)

- *Guidance for Directors – Dealing with Risk in the Boardroom,* 1999

  Sections cover:
  - introduction;
  - considering whether the organisation is in control;
  - reviewing information about future performance, opportunity and risk;
  - being aware and taking action.

  Appendices cover:
  - overview of CICA Criteria of Control framework;
  - the involvement of the board or directors in assessing the effectiveness of control;
  - approving the assessment;
  - contributing to the progress of the assessment; and
  - discussing the results of the assessment.

CIPFA (Further and Higher Education panel)

- *An Introductory Guide to Risk Management in Further and Higher Education,* 1999

  Provides a definition of risk management and risk assessment in the further and higher education sector and covers: aims of risk management; addressing risk management; and the process of risk management.

CIPFA (Technical Information Services Risk Management Working Group/ Financial Management Panel)

- *Risk management in the Public Services,* 2001

  Sections cover:
  - introduction to risk management;
  - the elements of successful risk management;
  - what is risk management?;
  - embedding risk management within the organisation;
  - identifying the risks;
  - assessing the likelihood and impact; and
  - determining the response and agreeing action.

CPA Australia

The CPA Australia's Public Sector Centre of Excellence recently released a series of publications to contribute to the sector's knowledge of risk management strategies and tools. The publications include:

- *A Research Report on Risk Management in the Public Sector;*
- *Public Sector Risk Management: A State of Play;*
- *Case Studies in Public Sector Risk Management;* and
- *Enterprise-Wide Risk Management: Better Practice Guide for the Public Sector*

Department of Trade and Industry, UK

- *Managing Business Risk,* 2001

  Seventy-seven pages, includes contemporary approaches to risk management, why risk management has risen up the corporate agenda, case study, corporate responses to specific risks (reputation; transaction; legal; technological; corporate tax; transfer pricing). In TIS collection, ref 658.155 MAN

- *Business Risk,* 2000

  Seventy-seven pages. Covers an overview of business risk, executive responsibility and risk, managing risk, e-business risk, risk in SMEs. In TIS collection ref 658.155 BUS

ICAEW

- *Risk Management for SMEs,* 2002

  This report aims to establish good practice for the management of risk, particularly among small and medium sized enterprises.

- *Working for Better Risk Reporting*

  A position paper that takes a leading role in promoting the idea that companies - particularly listed companies - should report on their major business risks and how management deals with them.

- *Internal Control – Guidance for Directors on the Combined Code (known as the Turnbull report),*1999

  This guidance is based on the adoption by a company's board of a risk-based approach to establishing a sound system of internal control and reviewing its effectiveness. This should be incorporated by the company within its normal management and governance processes. It should not be treated as a separate exercise undertaken to meet regulatory requirements.

ICAEW (Audit Faculty)

- *Risk Management and the Value Added by Internal Audit,* 2000

  Sections cover:
  - executive summary;
  - risk and risk management – an overview;
  - corporate governance and the Turnbull report;
  - the board and its committees;
  - the role and value of internal audit;
  - other review and compliance functions;
  - external audit and internal audit;
  - assessing the need for an internal audit function;
  - reviewing an internal audit function; and conclusion.

  Appendices cover:
  - assessing the need for an internal audit function; and
  - reviewing an internal audit function.

ICAEW (Centre for Business Performance)

- *Implementing Turnbull – A Boardroom Briefing*, 1999

  Intends to be practical guidance for directors, especially those of smaller listed companies.

ICAEW (Faculty of Finance and Management)

- *Business risk management,* 1999

  (Eleven page summary of *Business Risk Management*, a publication of the Faculty of Finance and Management, by J. Shackleton)

  Sections cover:
  - different types of risk;
  - why managing risks is important;
  - a practical guide to assessing business risk;
  - identifying risks;
  - measure the risk;
  - impact of risk;
  - deal with risks;
  - reporting risk;
  - creating a business continuity plan;
  - monitoring; and
  - examples of factors increasing risk levels.

ICAEW (Financial Reporting Committee)

- *No Surprises – the Case for Better Risk Reporting,* 1999

  Based on research into disclosures from companies which floated on the LSE in 1998. Appendices contain examples.

- *Financial Reporting of Risk*

  Outlines proposals for a statement of business risk (60 pages, PDF format). The appendices contain an Arthur Andersen business risk model and extracts from annual reports and listing particulars.

IFAC

- *International Management Accounting Practice Statement on Currency Exposure and Risk Management* (February 1996)

  Downloadable from IFAC website for registered users.

IFAC (Financial and Management Accounting Committee)

- *Enhancing Shareholder Wealth by better Managing Business Risk,* 1999

  This paper has been developed in response to this increasing demand for information on risk management issues. It is intended to extend awareness of some of the leading edge issues, provide practical guidance on best practice and convey current thought leadership in regard to risk management.

  Available on the IFAC website to registered users at: http://www.ifac.org/

Institute of Internal Auditors (UK)

- *Control and Risk Self-assessment,* 1999

- *Effective Governance – Practical Guidance on Implementing Risk Management and Internal Control Governance Requirements,* 1999

  Corporate governance requirements for all types of organisation in the UK are changing rapidly and many organisations are looking for guidance on how to interpret the internal control and risk management requirements to ensure that value is added to their organisation whilst, at the same time minimising cost and disruption. The first section of this publication reviews the progression of corporate governance across a range of private and public sector organisations over the last decade and also looks at the European perspective. Section 2 specifically focuses on the principles and provisions of the Combined Code, gives a summary of the Turnbull guidance and sets out the IIA's position as regards this guidance. Section 3 offers practical advice and section 4 focuses on five case studies: BG plc; Diageo plc; LIFFE; NatWest Group; and the NHS.

- *Professional Briefing Note 14*

  The main purpose of this Professional Briefing Note (PBN) is to explore how Control Risk Self Assessment (CRSA) has been used in practice and to offer advice and guidance to internal auditors who may become involved in such programmes. It also explores how internal audit may best be involved with such programmes without compromising its independence.

- *Managing Risk,* 1998
  Professional Briefing Note 13

  This Professional Briefing Note has three main objectives:
  - to outline the main characteristics of a risk-oriented approach to management;
  - to provide guidance on its implications for internal audit and on how internal auditors can align their work so that it supports such an approach; and
  - to provide advice on how a risk-oriented approach can be applied within internal audit.

KPMG

- *The KPMG Review of Internal Control: A Practical Guide*, 1999

- *Achieving Measurement Performance Improvement in a Changing World: The Search for New Insight*, KPMG Assurance and Advisory Services Centre, New York, 2002

- *Managing Business Risk*, joint business guide with the CBI, 2001

  The KPMG publications are available from www.KPMG.com and the CBI guide is available from the CBI.

Standards Australia

This website contains numerous resources in the risk management field and can be accessed on:

www.standards.com.au

UK National Audit Office

- *Supporting Innovation: Managing Risks in Government Departments,* HMSO, 2000

  A survey of all UK government departments (following distribution of a questionnaire to assess levels of risk management practice) and aims to promote good practice by giving case studies and examples from both the public and private sectors.

- *Accounts Commission for Scotland, Shorten the Odds*, 1999

  Audit Commission, Worth the Risk, 2001

  Both publications discuss good practice in risk management for local government bodies.